CONSAP
CONCESSIONARIA SERVIZI ASSICURATIVI PUBBLICI S.P.A.

MODELLO ORGANIZZATIVO PRIVACY

Ai sensi del Regolamento UE 2016/679

CONSAP CONCESSIONARIA SERVIZI ASSICURATIVI PUBBLICI S.P.A.

MODELLO ORGANIZZATIVO PRIVACY

Ai sensi del Regolamento UE 2016/679

SOMMARIO

1. PREMESSA 4
2. PRINCIPI GENERALI 5
2.1 DEFINIZIONE DEI PRINCIPI E DEI TERMINI FONDAMENTALI IN AMBITO PRIVACY 5
2.2 CRITERI ED INDIRIZZI 8
2.3 REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI (GDPR) 10
2.4 SISTEMA SANZIONATORIO 12
3. QUADRO NORMATIVO DI RIFERIMENTO 13
4. RUOLI E RESPONSABILITÀ IN AMBITO PRIVACY 14
4.1 DATA PROTECTION GOVERNANCE 14
4.2 IL TITOLARE DEL TRATTAMENTO 15
4.3 IL RESPONSABILE DEL TRATTAMENTO 15
4.4 L'AMMINISTRATORE DELEGATO 16
4.5 RESPONSABILI INTERNI DEL TRATTAMENTO 17
4.6 PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI 18
4.7 RESPONSABILI ESTERNI DEL TRATTAMENTO 21
4.8 RESPONSABILE PER LA PROTEZIONE DEI DATI (DATA PROTECTION OFFICER) 22
4.9 GLI AMMINISTRATORI DI SISTEMA 27
4.10 SERVIZIO AUDIT, COMPLIANCE, RISK MANAGEMENT E PRIVACY 27
5. POLICY DATA PROTECTION 27
6. REGISTRO DEL TRATTAMENTO DEI DATI 28
7. RISK ASSESSMENT PRIVACY 29
7.1 MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE 257
8. VALUTAZIONE D'IMPATTO - DATA PROTECTION IMPACT ASSESSMENT (DPIA) 273
9. REGOLAMENTI E PROCEDURE PRIVACY 273
9.1 REGOLAMENTO AMMINISTRATORI DI SISTEMA 273
9.2 INCIDENT MANAGEMENT 274
9.3 REGOLAMENTO DATA BREACH 275
9.4 REGOLAMENTO DIRITTI INTERESSATI 278
10. INFORMAZIONE E FORMAZIONE 279
11. GESTIONE E AGGIORNAMENTO DEL MOP 280

ALLEGATI

1. Policy Data Protection; 2. Regolamento amministratori di sistema; 3. Regolamento Individuazione e notificazione Data Breach; 4. Regolamento Esercizio dei diritti degli Interessati.

1. PREMESSA

Il presente **Modello Organizzativo *Privacy* (MOP)** raccoglie le misure tecniche ed organizzative che Consap S.p.A. attua per garantire - ed essere in grado di dimostrare - la conformità al Regolamento UE 2016/679 (di seguito brevemente "GDPR" o "Regolamento"), pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016. Nell'ordinamento italiano è, inoltre, successivamente intervenuto il Decreto Legislativo 10 agosto 2018, n. 101 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679", pubblicato in Gazzetta Ufficiale il 4 settembre 2018 ed entrato in vigore il 19 settembre 2018, allo scopo di coordinare la normativa comunitaria con il previgente Codice *Privacy* introdotto con il D.Lgs. n. 196/2003 e di dirimere le incertezze interpretative derivate dalla sovrapposizione delle norme, comunitarie da un lato e nazionali dall'altro, che costituiscono l'attuale quadro normativo.

L'adozione delle misure tecniche ed organizzative adeguate è imposta dagli artt. 24 e seguenti del GDPR, ai sensi dei quali le politiche interne e le misure da attuare per soddisfare i principi della protezione dei dati, devono tener conto, in concreto, della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento nonché del rischio per i diritti e le libertà delle persone fisiche interessate. Al fine di rispettare tale requisito, pertanto, l'elaborazione del presente modello ha richiesto l'esame della realtà aziendale e la valutazione dei rischi cui sono potenzialmente esposti gli interessati.

Pertanto, il Modello Organizzativo *Privacy* redatto da Consap S.p.A. ha lo scopo di racchiudere in unico documento le principali misure, procedure e regolamenti adottate dalla Società al fine di tutelare i dati personali in conformità al Regolamento Generale sulla Protezione dei Dati.

Il presente documento trova applicazione nei confronti di tutto il personale di Consap, vale a dire i dipendenti (per tali intendendosi tutti coloro che sono legati alla Società da un rapporto di lavoro subordinato quali impiegati, quadri, funzionari e dirigenti di ogni ordine e grado), i collaboratori, nonché ai componenti degli organi amministrativi e di controllo, per quanto di competenza di ciascuno di essi.

2. PRINCIPI GENERALI

2.1 DEFINIZIONE DEI PRINCIPI E DEI TERMINI FONDAMENTALI IN AMBITO PRIVACY

Ai sensi della normativa di riferimento e ai fini del presente Modello Organizzativo *Privacy*, s'intende per[1]:

- ***«Dato personale»***, oppure ***«dato»***: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

- ***«Trattamento»***: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- ***«Limitazione di trattamento»***: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

- ***«Profilazione»***: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

- ***«Pseudonimizzazione»***: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate

[1] I termini non previsti dal presente paragrafo avranno il significato ad essi attribuito nel Regolamento UE 2016/679 e nella normativa nazionale di riferimento.

separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

- ***«Archivio»***: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

- ***«Titolare del trattamento»***: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

- ***«Responsabile del trattamento»***: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;

- ***«Autorizzati / designati al trattamento»***: le persone fisiche, espressamente designate, autorizzate a compiere, mediante l'attribuzione di specifici compiti e funzioni, operazioni di trattamento dal titolare o dal responsabile, sotto la loro autorità (ex "incaricati");

- ***«Destinatario»***: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

- ***«Terzo»***: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

- ***«Consenso dell'interessato»***: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali

che lo riguardano siano oggetto di trattamento;

- ***«Violazione dei dati personali»***: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

- ***«Dati genetici»***: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

- ***«Dati biometrici»***: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

- ***«Dati relativi alla salute»***: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

- ***«Impresa»***: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le Società di persone o le associazioni che esercitano regolarmente un'attività economica;

- ***«Norme vincolanti d'impresa»***: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

- ***«Autorità di controllo»***: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento: per l'Italia, il Garante per la Protezione dei dati personali, istituito con la Legge n. 675/1996;

- ***«Amministratore di Sistema»***: la persona fisica a cui è conferito il compito di sovrintendere alla gestione e alla manutenzione di un Sistema di elaborazione (a titolo

esemplificativo, gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi *software* complessi): si tratta, dunque, di una figura professionale che approfondisce le competenze di un tecnico *hardware* e *software* soprattutto per quanto riguarda le caratteristiche delle architetture informatiche e, in particolare, l'utilizzo e la condivisione di grandi quantità di dati attraverso le reti di comunicazione. Si occupa essenzialmente di ogni tipo di rete informatica, comprese quelle a cui non si accede via *web*, come le reti *intranet* e implementa i sistemi di sicurezza del *networking* e definisce le procedure di autenticazione alla rete e di autorizzazione all'accesso ai dati da parte gli utenti, curando interventi di conservazione dei dati attraverso debite soluzioni di *backup* e progettando le attività di supporto al *disaster recovery*;

- ***«Misure di sicurezza»***: le misure tecniche e organizzative adeguate a garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente alla normativa vigente;

- ***«Registro delle attività di trattamento»***: il registro, tenuto da ciascun titolare e/o responsabile, delle attività di trattamento svolte sotto la propria responsabilità, ovvero, nel caso del responsabile del trattamento, delle attività svolte per conto di un titolare del trattamento;

- ***«Comunicazione»***: indica il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o interconnessione;

- ***«Diffusione»***: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

2.2 CRITERI ED INDIRIZZI

La Società adotta misure organizzative per essere in grado di dimostrare in ogni momento il rispetto delle norme in materia e, in particolare dei seguenti principi fondamentali indicati dall'Art. 5 del GDPR:

a) *liceità, correttezza e trasparenza*: i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
b) *limitazione della finalità* - raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
c) *minimizzazione dei dati* - adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
d) *esattezza*: esatti e, se necessario, aggiornati;
e) *limitazione della conservazione*: conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
f) *integrità e riservatezza*: trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

L'osservanza di tali principi è assicurata con l'adozione di misure tecniche e organizzative adeguate atte a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente alla normativa sin dalla progettazione e con misure di protezione per impostazione predefinita (artt. 24,25 e 26 GDPR) nonché per gestire in maniera trasparente il rapporto con gli interessati mettendoli in condizione di esercitare i propri diritti in maniera rapida ed efficace.
I dati personali vengono trattati esclusivamente allo scopo di consentire alla Società di svolgere la propria attività, nel rispetto delle previsioni normative che disciplinano i Fondi e i servizi che le sono affidati dalle Pubbliche Amministrazioni di riferimento e di adempiere gli obblighi di legge a cui Consap è soggetta (come soggetto di diritto privato controllato interamente dal Ministero dell'Economia e delle Finanze), in particolare quelli in materia di trasparenza, prevenzione della corruzione, responsabilità amministrativa degli enti e quelli riguardanti la gestione dei rapporti di lavoro e dei rapporti societari. Le operazioni di trattamento dei dati personali svolte da Consap includono la raccolta, registrazione, organizzazione, consultazione, utilizzo, elaborazione, conservazione, archiviazione, trasmissione, limitazione e cancellazione di dati personali.

2.3 REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI (GDPR)

Il GDPR è costituito da tre principi ispiratori, che permeano e sostengono l'intero impianto normativo ed il cui rispetto è protetto da un sistema sanzionatorio, delineato dagli artt. 83 e ss. del Regolamento. Tali principi essenziali sono quelli di:

1) ***accountability***, ossia il principio di responsabilizzazione: il Regolamento non effettua una tipizzazione puntuale delle misure tecniche e organizzative, esprimendosi unicamente in termini di loro adeguatezza al rischio "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche" (art. 32 GDPR). Si tratta di una innovazione profonda in quanto viene attribuito ai Titolari il compito di decidere autonomamente le modalità, le garanzie ed i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative ed alla luce di alcuni criteri specifici indicati nel Regolamento. Ciò impone un approccio integrato, che interessi tutte le aree aziendali, concreto e *risk-based* e che dia luogo a comportamenti proattivi;

2) ***privacy by design*****,** che impone l'adozione di misure di protezione fin dalla fase di progettazione del trattamento;

3) ***privacy by default***, che prescrive un utilizzo che si limiti, per impostazione predefinita, ai soli dati necessari a rispondere alle finalità specifiche della gestione dei dati.

Tali principi si traducono nell'assunto in base al quale ogni trattamento di dati personali debba avvenire, potendolo dimostrare anche *ex post*, nel rispetto dei principi fissati all'articolo 5 del Regolamento. In particolare, il trattamento è lecito allorché trovi fondamento in una idonea base giuridica (art. 6 GDPR).
L'interessato deve avere a disposizione una procedura efficace e accessibile per consentirgli di ottenere l'accesso ai suoi dati in un tempo ragionevole, e quindi di conoscere "se" e "quali" dati siano eventualmente detenuti dal titolare, "perché" e "come li abbia avuti". A livello operativo, tali principi si concretizzano nelle seguenti azioni:
a) adempimento dell'obbligo preventivo di informativa (artt. 13 e 14 GDPR), da rendere sempre ed obbligatoriamente, tutte le volte in cui debba essere iniziato il trattamento, non necessariamente per iscritto ma con forme documentabili ex post;
b) istituzione del Registro delle attività di trattamento (art. 30 GDPR) che costituisce il

punto di partenza per la predisposizione dell'intero impianto documentale, deputato a raccogliere le evidenze, i controlli ed i processi che consentono di soddisfare l'accountability del sistema *privacy*;

c) designazione dei Responsabili del trattamento (art. 28 Reg.), indispensabile a legittimare tutti i soggetti terzi che effettuano trattamenti di dati personali per conto del titolare, che devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che i trattamenti soddisfino i requisiti del Regolamento e garantiscano la tutela dei diritti dell'interessato;

d) formazione ed autorizzazione dei soggetti incaricati, interni alla struttura del titolare e/o al responsabile che, agendo sotto la loro autorità, hanno accesso ai dati (art. 29 GDPR). Fondamentale rilievo assume, in proposito, lo svolgimento di specifiche attività di formazione ed informazione a beneficio di tutti i soggetti autorizzati come verrà approfondito nei paragrafi successivi;

e) designazione del Responsabile della protezione dei dati personali (*Data Protection Officer*, artt. 37-39 GDPR) intesa come figura fondamentale che deve raccogliere in sé competenze normative, tecniche, comunicative e di conoscenza profonda della struttura e dell'organizzazione aziendale;

f) formalizzazione della disciplina del processo di *data breach*, (artt. 33 e 34 GDPR) ossia della violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, la cui predisposizione consente una gestione tempestiva e ponderata dell'evento e delle sue conseguenze, compresa la notifica all'Autorità Garante.

L'obiettivo del presente Modello Organizzativo *Privacy* è di garantire e dimostrare che il trattamento dei dati personali da parte di Consap S.p.A. avviene in modo lecito, corretto e trasparente. Tale obiettivo è conseguibile attraverso la realizzazione di una gestione interna ben strutturata che promuova la cultura della *privacy* e della sicurezza dei dati personali, consolidando i principi comportamentali idonei a garantire la trasparenza, la sicurezza e la correttezza dei trattamenti. Con l'ulteriore conseguenza di evitare la possibile erogazione delle sanzioni amministrative pecuniarie di cui all'art. 83 GDPR nonché di quelle penali di cui al vigente D. Lgs. n. 196/2003 potendo, con la sua adozione, dimostrare l'attuazione concreta, efficiente ed efficace delle misure tecniche ed

organizzative adeguate alla protezione dei dati personali da essa trattati, direttamente o tramite soggetti terzi che li effettuano per suo conto.

2.4 SISTEMA SANZIONATORIO

In caso di violazione delle disposizioni previste dal Regolamento da parte di Consap, l'Autorità di controllo ha il potere di infliggere sanzioni amministrative pecuniarie e di fissare l'ammontare delle stesse fino ad un massimo di 20 milioni di euro o fino al 4% del fatturato totale annuo dell'esercizio precedente. Nel dettaglio, il Regolamento disciplina direttamente le sanzioni amministrative pecuniarie e prevede sanzioni fino a:

a) 10 milioni di euro, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nei casi in cui si verifichino violazioni di obblighi del Titolare o del Responsabile del trattamento, obblighi dell'organismo di certificazione, nonché obblighi dell'organismo di controllo.

b) 20 milioni di euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nei casi in cui si verifichino violazioni di diposizioni relative a principi base del trattamento, diritti degli interessati, trasferimento dei dati personali in paesi terzi o verso organizzazioni internazionali, nonché inosservanza di un ordine, limitazione provvisoria o definitiva o di un ordine di sospensione dei flussi da parte dell'autorità di controllo.

Le sanzioni amministrative possono essere inflitte sia a persone fisiche che giuridiche, inclusi i Titolari e i Responsabili del trattamento, il *Data Protection Officer* (DPO) e gli organismi di certificazione e monitoraggio.
Per quanto riguarda, invece, le violazioni riscontrate da parte del personale della Società alla *Policy*, alle procedure in materia di *data protection*, alle istruzioni ricevute per il trattamento dei dati personali e alle disposizioni normative di riferimento, esse sono sanzionate mediante l'applicazione delle misure previste dal Sistema disciplinare interno, nel rispetto del C.C.N.L. di riferimento.

3. QUADRO NORMATIVO DI RIFERIMENTO

- Regolamento generale sulla protezione dei dati personali (GDPR, *General Data Protection Regulation* - Regolamento UE 2016/679) pubblicato nella Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno, avente efficacia negli Stati membri dell'Unione europea a partire dal 25 maggio 2018;
- Linee Guida e altra documentazione pubblicata dal Gruppo dei Garanti dell'Unione Europea (cd. "WP29") ex art. 29 della direttiva 95/46;
- Decreto legislativo 30 giugno 2003, n. 196, recante il Codice per la protezione dei dati personali, come modificato dal Decreto Legislativo 10 agosto 2018, n. 101;
- Decreto legislativo 10 agosto 2018, n. 101 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- Decreto legislativo del 4 settembre 2024, n. 138;
- Trattato sul funzionamento dell'Unione Europea (TFUE);
- Carta dei diritti fondamentali dell'Unione Europea;
- ISO / IEC 27001:2017: *Information Technology – Security techniques – Information Security Management Systems – Requirements*;
- UNI ISO 31000:2010 – *Risk Management – Principles and Guidelines*;
- UNI EN ISO / IEC 9001: 2015 – *Quality Management System – Requirements*;
- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema, emanate dall'Autorità Garante *Privacy* il 27 novembre 2008.

4. RUOLI E RESPONSABILITÀ IN AMBITO PRIVACY

4.1 DATA PROTECTION GOVERNANCE

La normativa individua le principali figure organizzative che vengono in rilievo, ai fini *privacy*, per garantire che lo svolgimento delle varie attività aziendali avvenga nel rispetto dei criteri di corretta gestione e protezione dei Dati Personali. Le predette figure sono:

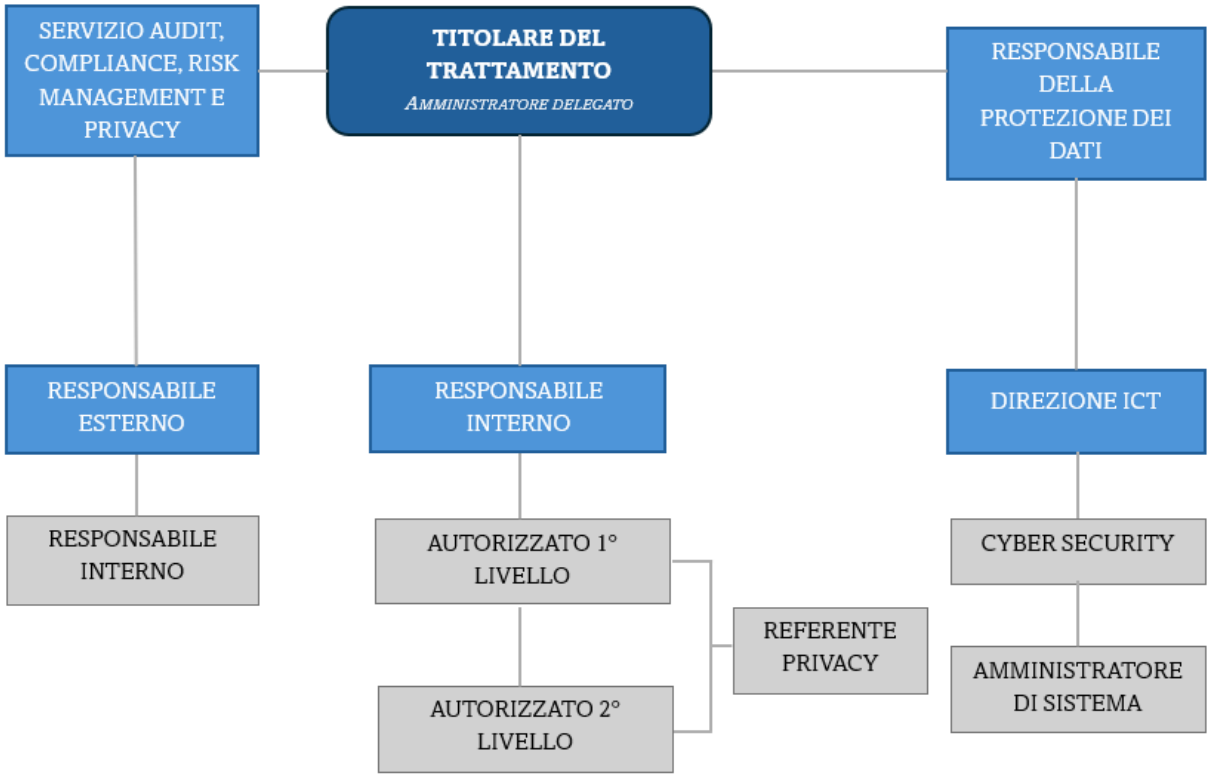
a) il Titolare del trattamento;
b) il Responsabile del trattamento;
c) il Responsabile della Protezione dei Dati personali (*Data Protection Officer*, DPO);
d) i Soggetti autorizzati al trattamento;
e) gli Amministratori di Sistema.

Al fine di calare le predette figure all'interno della propria realtà aziendale e del contesto in cui opera, Consap ha adottato e implementato un proprio modello organizzativo, nel quale le diverse funzioni e unità organizzative aziendali – come individuate in virtù dell'organigramma generale attualmente vigente – vengono valorizzate nell'ambito del sistema di *data protection*, mediante attribuzione di compiti, responsabilità e poteri diversi e specifici, parametrati al ruolo e alle mansioni proprie di ciascuno dei soggetti preposti alle operazioni di trattamento o, comunque, coinvolti nella gestione degli adempimenti normativi. Si indicano, di seguito, i principali ruoli previsti da Consap, in qualità sia di Titolare sia di Responsabile del trattamento, che delineano l'organigramma *privacy*:

- Amministratore Delegato;
- Responsabili interni del trattamento;
- Autorizzati al trattamento di I livello;
- Autorizzati al trattamento di II livello;
- Referenti *Privacy*;
- Responsabili esterni del trattamento;
- Sub-Responsabili;
- Responsabile della Protezione dei Dati Personali – *DPO*;
- Servizio *Audit, Compliance, Risk management e Privacy*;
- Direzione ICT;
- Amministratori di sistema.

Graficamente si può rappresentare come di seguito:

**Organigramma privacy*



4.2 IL TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali.

Consap assume la qualifica di Titolare, con riferimento ad alcune attività di trattamento, provvedendo alla determinazione dei mezzi e delle finalità di trattamento (salve le ipotesi in cui finalità e mezzi siano già determinate da atti normativi): su di essa, conseguentemente, incombono tutti gli obblighi e le responsabilità che la normativa, europea e nazionale, impone al Titolare: primo fra tutti, l'obbligo di mettere in atto, riesaminare e aggiornare le misure tecniche ed organizzative adeguate, per garantire – ed essere in grado di dimostrare – che il trattamento di dati personali viene effettuato dalla Società conformemente al Regolamento (UE) 2016/679 e al D. Lgs. n. 196/2003.

4.3 IL RESPONSABILE DEL TRATTAMENTO

Il Regolamento all'art. 28 identifica nel Responsabile del trattamento la persona fisica o giuridica che tratta i dati personali per conto del Titolare. I Responsabili del trattamento rispondono per il danno causato dal trattamento solo se non hanno adempiuto gli obblighi del Regolamento specificatamente loro diretti o se hanno agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare del trattamento; lo stesso vale per i sub-Responsabili nei confronti del Responsabile, ferma restando la responsabilità di quest'ultimo nei confronti del Titolare (anche per la condotta posta in essere dal sub-Responsabile). Rispondono, inoltre, delle sanzioni amministrative pecuniarie irrogabili dall'Autorità Garante secondo gli stessi termini e modalità del Titolare del trattamento. Sono esonerati dalla responsabilità per danni se dimostrano che l'evento dannoso non è in alcun modo loro imputabile. Consap assume tale veste rispetto ai trattamenti di dati personali effettuati, talvolta, nell'ambito delle Convenzioni in essere, per conto delle Pubbliche Amministrazioni di riferimento; la Società può, inoltre, avvalersi di soggetti esterni che, nell'ambito dei servizi di *outsourcing* prestati in favore della stessa, effettuano trattamenti di dati personali, presentando garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che i trattamenti stessi soddisfino i requisiti del Regolamento e garantiscano la tutela dei diritti dell'interessato.

Il Regolamento prevede che il Responsabile del trattamento presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate: a tal fine, Consap si impegna in proprio – in qualità di Responsabile del trattamento – a rispettare le previsioni normative in parola e, per quanto concerne gli outsourcer di cui si avvale, a valutare l'adeguatezza dei Responsabili del trattamento, rispetto ai suddetti requisiti, e disciplina contrattualmente i termini e le condizioni relativi al trattamento dei dati personali affidati.

4.4 L'AMMINISTRATORE DELEGATO

Per lo svolgimento degli adempimenti e degli obblighi in materia di protezione dei dati personali, il Consiglio di Amministrazione delega l'Amministratore Delegato. L'Amministratore Delegato nell'ambito dei poteri delegati:

a) designa i Responsabili interni ed esterni del Trattamento;
b) nomina il Responsabile per la protezione dei dati personali (DPO);
c) nomina gli Amministratori di sistema;

d) sottoscrive, per accettazione, gli atti di nomina di Consap quale Responsabile del Trattamento;
e) notifica al Garante per la protezione dei dati personali gli eventuali *data breach* al ricorrere dei presupposti normativi;
f) irroga le eventuali sanzioni disciplinari;
g) garantisce attraverso la struttura organizzativa l'esercizio dei diritti degli interessati di cui agli artt. da 13 a 18 del GDPR.

4.5 RESPONSABILI INTERNI DEL TRATTAMENTO

La Società ha deciso di nominare, mediante apposito atto, dei Responsabili (interni) del trattamento, individuati nei Dirigenti delle Direzioni aziendali o nei Titolari di Servizio per le funzioni in *staff* che svolgono attività che comportano il trattamento dei dati personali, con il compito di fornire supporto e ausilio al DPO nell'adempimento degli obblighi che la normativa pone in capo alla Società - vuoi come Titolare, vuoi come Responsabile del trattamento - sulla base delle istruzioni fornite dal Titolare (o dal Responsabile) stesso. I Responsabili interni hanno visibilità su tutti i dati trattati all'interno della propria Direzione e, per quanto di propria competenza e per il personale loro assegnato, sono tenuti al rispetto della riservatezza, integrità e qualità dei dati e ad utilizzarli esclusivamente per le finalità specificate nell'ambito delle attività assegnate.

Ad essi spetta l'attuazione ed il controllo sulle misure tecniche e organizzative individuate da Consap per garantire un livello di sicurezza dei trattamenti adeguato al rischio di volta in volta valutato, ai sensi dell'art. 32 del Regolamento. In particolare, i Responsabili interni del trattamento sono tenuti a:

a) informare il DPO, senza ingiustificato ritardo, dei casi di violazione dei dati personali di cui vengano a conoscenza nello svolgimento della propria attività, per la successiva eventuale notifica della violazione all'Autorità di controllo;
b) soddisfare le richieste avanzate da parte dell'Amministratore Delegato, per rendere effettiva ed efficace l'adozione delle misure tecniche ed organizzative individuate dalla Società;
c) fornire al DPO tutte le informazioni necessarie alla predisposizione e al successivo aggiornamento dei Registri delle attività di trattamento;

d) informare tempestivamente il DPO nei casi di nuovi trattamenti posti in essere, ovvero delle variazioni di rilievo a quelli esistenti che comportino la necessità di apportare modifiche al Registro delle Attività di trattamento;
e) provvedere, anche per il tramite dei loro sottoposti, a dare tempestivo riscontro alle richieste per l'esercizio dei diritti degli interessati pervenute;
f) controllare le attività poste in essere e i comportamenti tenuti dagli autorizzati del trattamento (di I e di II livello) all'interno della propria Direzione di competenza;
g) comunicare al Titolare (nel caso in cui per lo svolgimento delle attività Consap rivesta il ruolo di Responsabile del trattamento) ogni variazione intervenuta riguardante l'aggiunta o la sostituzione di Responsabili esterni del trattamento (fornitori di beni e servizi).

4.6 PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Il personale autorizzato al trattamento dei dati include coloro che sono espressamente designati da Consap a compiere le materiali operazioni di trattamento dei dati personali, inclusa la raccolta, l'elaborazione (tramite i sistemi applicativi o manualmente), l'archiviazione, la comunicazione e la diffusione. Tale personale è rappresentato esclusivamente da persone fisiche ed individuato e classificato in base alle seguenti tipologie:

a) Autorizzati al trattamento di I livello, vale a dire i Titolari di Servizio, di supporto ai Responsabili interni che garantiscono il presidio delle operazioni di trattamento nelle attività quotidiane;
b) Autorizzati al Trattamento di II livello, vale a dire gli altri dipendenti assegnati al Servizio, che trattano dati personali;
c) Referenti *privacy*, i referenti individuati all'interno di ciascun Servizio con il compito di effettuare tutte le operazioni di trattamento come (a titolo esemplificativo) compilare il Registro dei trattamenti, redigere la DPIA, predisporre e aggiornare le informative *privacy*.

La nomina di tali soggetti avviene per iscritto e deve essere riscontrata dall'autorizzato per presa visione. Gli autorizzati al trattamento trattano esclusivamente i dati necessari per lo svolgimento delle attività ad essi assegnate nell'ambito delle Direzioni / Servizi / Settori autonomi di appartenenza, compiendo le sole operazioni di trattamento a ciò

strumentali, nel rispetto delle disposizioni del Regolamento e delle regole contenute nella *Policy* e nelle Procedure *Data Protection* adottate dalla Società.
Gli autorizzati sono soggetti ad apposito vincolo di riservatezza derivante, oltre che dal contratto di lavoro ai sensi di quanto previsto dalle norme civilistiche, ove applicabile, anche dagli atti di nomina al trattamento di dati personali (in base alle tipologie suindicate), consegnate dai Responsabili interni (Dirigente responsabile della Direzione), prima che il soggetto inizi la propria attività di trattamento dei dati.

Autorizzati al trattamento di I livello.

I soggetti in parola hanno visibilità sui dati personali trattati nell'ambito delle funzioni e compiti a loro affidati. Essi sono tenuti a:

- sovraintendere all'implementazione delle misure organizzative, operative e tecniche in materia di protezione dei dati personali;
- vigilare sull'osservanza generale delle norme in materia di privacy così come prescritto dalle disposizioni regolamentari in materia di compiti dei Responsabili/Titolari delle Unità Organizzative, in conformità alle norme vigenti, alle direttive ricevute dai superiori livelli gerarchici ed alle specifiche istruzioni contenute nelle lettere di autorizzazione al trattamento dei dati;
- coordinare e supervisionare le attività svolte dagli addetti anch'essi in qualità di autorizzati da Consap al trattamento di dati, con riferimento a tutti i profili attinenti al trattamento e alla protezione dei dati personali, nonché all'adempimento degli obblighi normativi posti in capo al Titolare e al Responsabile del trattamento, in particolare per quanto concerne l'esercizio dei diritti da parte degli interessati;
- segnalare al DPO la necessità di apportare eventuali modifiche/integrazioni al Registro dei Trattamenti;
- riportare al Servizio *Audit, Compliance, Risk Management* e *Privacy* e/o al DPO per tutte le questioni attinenti alla protezione dei dati personali, in particolare per quanto concerne la conformità delle attività di trattamento alla normativa vigente e la corretta applicazione di procedure e policy a tal fine definite dalla Società.

Autorizzati al trattamento di II livello

I soggetti in parola hanno visibilità sui dati personali trattati nell'ambito delle funzioni e compiti a loro affidati. Essi sono tenuti a:

- osservare e applicare le misure organizzative, operative e tecniche in materia di trattamento protezione dei dati personali;
- svolgere le attività in conformità alle disposizioni normative attualmente vigenti in materia di trattamento e protezione dei dati personali, nonché nel rispetto delle direttive ricevute dai superiori livelli gerarchici ed alle specifiche istruzioni contenute nelle lettere di autorizzazione al trattamento dei dati consegnate dai Responsabili interni;
- cooperare, per quanto di competenza, con le funzioni preposte nello svolgimento delle attività necessarie ad assicurare l'adempimento degli obblighi normativi posti in capo al Titolare e al Responsabile del trattamento, in particolare per quanto concerne l'esercizio dei diritti da parte degli interessati;
- segnalare al Titolare del Servizio eventuali criticità / anomalie / difformità delle attività di trattamento, riscontrate nello svolgimento delle ordinarie attività lavorative, rispetto alle previsioni normative e/o alle procedure e regolamenti interni adottati dalla Società.

Referenti Privacy

I referenti *privacy* sono gli interlocutori privilegiati del DPO aziendale, sono individuati all'interno di ogni Direzione o Servizio (per i Sevizi in staff), hanno visibilità sui dati personali trattati nell'ambito della Direzione o Servizio e sono nominati dai Responsabili di Direzione o dai Titolari di Servizio (per i Sevizi di *staff*).

I referenti *privacy* hanno il compito di fornire il supporto necessario al Responsabile Interno per assicurare il corretto adempimento in relazione agli obblighi normativi in materia di *privacy*, avvalendosi della consulenza del Responsabile della protezione dati aziendale. In particolare:

- danno concreta attuazione alle misure organizzative, operative e tecniche in materia di trattamento dei dati personali adottate dal Responsabile di primo livello;
- assicurano l'adempimento degli obblighi normativi posti in capo al Titolare e al Responsabile del trattamento, anche per ciò che concerne l'esercizio dei diritti da parte degli interessati:
- aggiornano per conto del Responsabile interno il Registro dei trattamenti anche attraverso l'utilizzo di appositi *tool* a ciò preposti;
- predispongo, unitamente al DPO, ove necessario, la DPIA;
- predispongono, aggiornano e archiviano le informative *privacy*;

- predispongono, unitamente al DPO, le nomine dei soggetti autorizzati di primo e secondo livello;
- predispongono, unitamente al DPO, le nomine dei Responsabili esterni del trattamento ex art. 28 GDPR;
- sono membri del Team che gestisce eventuali situazioni di *Data Breach*;
- partecipano a riunioni ogni qualvolta si introduca una nuova tecnologia o debbano essere attuate campagne o operazioni che riguardino il trattamento dei dati personali o si introducano nuove misure sulla sicurezza o potenziali sistemi di controllo a distanza dei dipendenti o qualora si vogliano applicare politiche che impattano sulla riservatezza dei dipendenti;
- conservano e archiviano la documentazione richiesta dal GDPR;
- supportano il DPO nel predisporre e tenere sotto controllo il piano delle attività previste;
- supportano il DPO nel pianificare e condurre le attività di *audit* (sia di conformità al GDPR che relativi all'applicazione delle procedure interne che impattano sul GDPR);
- tengono sotto controllo lo stato di avanzamento delle eventuali criticità emerse nel corso *dell'audit*;
- supportano il DPO nel tenere sotto controllo lo stato di avanzamento delle misure pianificate per la mitigazione dei rischi.

Il Referente *Privacy* ha l'obbligo di partecipare alle iniziative formative in materia di trattamento dei dati proposte dal Titolare del trattamento ai sensi dell'art 29 del Reg. UE 2016/679.

4.7 RESPONSABILI ESTERNI DEL TRATTAMENTO

Per Consap, i Responsabili esterni del trattamento sono individuabili sostanzialmente in fornitori terzi ai quali la Società si affida per il trattamento dei dati personali. I fornitori terzi possono, quindi, assumere la veste di Responsabili o di sub-responsabili, a seconda dell'ambito operativo di riferimento di Consap, ovvero a seconda che le attività in capo a Consap siano svolte in qualità di Titolare oppure di Responsabile.

Il Regolamento prevede che il Responsabile del trattamento presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate rispetto ai requisiti definiti dal Regolamento medesimo.

A tal fine, la Società si impegna a valutare l'adeguatezza dei Responsabili esterni del

trattamento, rispetto ai suddetti requisiti; tali requisiti sono previsti da specifiche clausole contrattuali e misure di sicurezza.
Nel caso in cui, nell'ambito delle attività affidate dalla Società a società esterne o a terzi affidatari di servizi, vengano trattati dati personali, il Responsabile interno del trattamento di riferimento richiede preliminarmente un parere al DPO circa il corretto inquadramento del terzo come Responsabile esterno del trattamento.
Qualora il DPO abbia confermato che sussistono le condizioni per designare il terzo come Responsabile esterno del trattamento (a titolo meramente esemplificativo, operano come Responsabili esterni del trattamento per conto e su istruzioni di Consap, società di archiviazione e di postalizzazione, società di *call center*, ecc.) i Responsabili interni del trattamento attivano le competenti funzioni aziendali affinché sia formalizzato l'atto di designazione e fornite le relative istruzioni in ordine al trattamento dei dati personali, condividendone preventivamente i contenuti con il DPO.
Nel caso in cui la Società sia designata quale Responsabile del trattamento e ricorra a fornitori esterni, la Società stessa si impegna a nominare questi ultimi responsabili esterni del trattamento ai sensi dell'art. 28 del regolamento mediante apposito atto formale, imponendo agli stessi i medesimi obblighi per la protezione dei dati imposti dal Titolare ed a comunicare a quest'ultimo ogni variazione intervenuta riguardante l'aggiunta o la sostituzione di altri fornitori di beni e servizi. I responsabili interni del trattamento garantiscono inoltre che i responsabili esterni non ricorrano ad altri sub-fornitori se non previa ed espressa autorizzazione del Titolare del trattamento dei dati.

4.8 RESPONSABILE PER LA PROTEZIONE DEI DATI (*DATA PROTECTION OFFICER*)

Il DPO (*Data Protection Officer* o RPD, Responsabile della Protezione dei Dati) è una figura introdotta dal GDPR con la funzione di affiancare il Titolare del trattamento, addetti e responsabili del trattamento affinché conservino i dati e gestiscano i rischi seguendo i princìpi e le indicazioni del Regolamento europeo. Il DPO è quindi un consulente tecnico e legale, costituendo anche l'interlocutore privilegiato del Garante per la protezione dei dati personali, con il quale è tenuto a cooperare. Nello specifico, l'art. 39 del Regolamento individua i seguenti compiti del DPO:

a) informare e fornire consulenza al Titolare o al Responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal

Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati personali nonché alle politiche del Titolare o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne l'attuazione ai sensi dell'art. 35 del Regolamento;
d) cooperare con l'autorità di controllo;
e) fungere da punto di contatto con l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del Regolamento, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Il DPO è designato in funzione delle qualità professionali e della capacità di assolvere i compiti sopra indicati: può essere, alternativamente, un componente interno, oppure esterno, alla Società, purché rispetti i requisiti richiesti dalla normativa. Requisiti e caratteristiche:

- professionalità e competenza;
- imparzialità, autonomia e indipendenza (assenza di conflitto di interessi e dotazione di *budget*);
- continuità di azione: coinvolgimento tempestivo e adeguato in tutte le questioni che riguardano il trattamento di dati personali (vigilanza, supporto valutativo, consulenza operativa).

Il DPO opera in *staff* al Titolare del trattamento ed è nominato dall'Amministratore delegato: è organo interno alla Società (anche quando l'incarico venga svolto da un soggetto esterno), che riferisce direttamente al Vertice aziendale; ove richiesto, svolge altresì un'attività di raccordo tra Consap e l'Autorità Garante sull'osservanza del Regolamento. L'assegnazione di compiti al DPO, in particolare quello di controllare il rispetto del GDPR e delle politiche aziendali in materia di protezione dei dati personali, non implica che il DPO sia personalmente responsabile della mancata osservanza: infatti, spetta sempre al Titolare mettere in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento dei dati è effettuato

conformemente al GDPR. La nomina del DPO, peraltro, costituisce a sua volta l'attuazione di una delle misure in questione. Per assolvere ai propri compiti, il DPO deve essere prontamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali: in particolare, per quanto concerne la valutazione d'impatto, il DPO deve essere obbligatoriamente consultato e coinvolto fin dalle fasi iniziali. Ciò significa che occorre garantire che:

- il DPO sia invitato a partecipare su base regolare alle riunioni del *management* di alto e medio livello;
- la presenza del DPO ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati personali, facendo in modo che il DPO disponga tempestivamente di tutte le informazioni pertinenti, in modo da poter rendere una consulenza adeguata;
- il parere del DPO sia sempre preso adeguatamente in considerazione: in caso di disaccordo con il parere espresso dal DPO, è buona prassi documentare le motivazioni che hanno portato a decisioni o condotte difformi da quelle raccomandate dal DPO;
- il DPO sia consultato tempestivamente qualora si verifichi una violazione di dati personali o altro incidente.

Il DPO può, altresì, essere contattato direttamente dagli interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei diritti riconosciutigli dal Regolamento.

Consap ha nominato un proprio Responsabile per la protezione dei dati, con l'obiettivo di ottenere il supporto necessario ad assicurare l'adeguatezza e l'effettività del sistema di *data protection* adottato: in particolare, sono state affidate al DPO:

a) attività di supporto, consulenza e indirizzo nei confronti delle Direzioni / Servizi aziendali;
b) attività di vigilanza sull'osservanza del Regolamento, delle altre disposizioni normative in materia di trattamento e protezione dei dati personali, delle politiche interne;
c) attività di informazione e formazione del personale;
d) attività di rappresentanza della Società, nei rapporti con i soggetti terzi e con il Garante per la protezione dei dati personali, limitatamente a quanto concerne le tematiche rilevanti ai fini *privacy*.

Il DPO ha un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno di Consap, e contribuisce a dare attuazione a elementi essenziali del Regolamento quali i principi fondamentali del trattamento, i diritti degli interessati, la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita, i registri delle attività di trattamento, la sicurezza dei trattamenti e la notifica e comunicazione delle violazioni di dati personali. Il DPO, segnatamente, collabora con le competenti strutture aziendali, affinché la Società possa adempiere agli obblighi previsti dalla normativa di riferimento:

- vigilando sul rispetto della normativa in materia di protezione dei dati personali, valutando l'adeguatezza e l'efficacia delle misure organizzative adottate, verificando l'aderenza dei comportamenti a politiche, piani, procedure, leggi e regolamenti;
- identificando le disposizioni normative applicabili alla Società e valutando l'impatto di eventuali mutamenti nel quadro di riferimento sulle procedure e sui processi aziendali vigenti;
- monitorando il costante aggiornamento e l'effettiva attuazione del sistema di *data protection* all'interno della Società, anche in termini di conformità delle relative previsioni alle procedure e alle prassi operative aziendali;
- prestando consulenza in materia di protezione dei dati personali, anche attraverso il rilascio di pareri, a tutte le Direzioni / Servizi aziendali coinvolti;
- offrendo supporto nella predisposizione e revisione di *Policy* e procedure in materia di *data protection*, nonché nella definizione di istruzioni operative per il trattamento;
- contribuendo alla conduzione delle Valutazioni d'impatto sulla protezione dei dati, ove necessario, e allo svolgimento delle verifiche di natura tecnica a seguito di eventuale *data breach*;
- curando, anche attraverso il supporto di consulenti esterni e con la collaborazione delle competenti strutture aziendali, l'istituzione iniziale, la conservazione e l'aggiornamento periodico del Registro delle attività di trattamento;
- curando l'informazione e la formazione del personale in tema di *data protection*;
- cooperando, all'occorrenza, con il Garante per la Protezione dei dati personali, con cui intrattiene le necessarie ed opportune relazioni, per questioni connesse al trattamento dei dati personali.

Nell'eseguire i propri compiti, il DPO:

- considera debitamente i rischi connessi al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo;
- svolge i controlli acquisendo informazioni per individuare i trattamenti svolti, e ne verifica la conformità;
- segnala le criticità rilevate e suggerisce al Titolare del trattamento gli interventi di miglioramento da attuare;
- è tenuto al segreto e alla riservatezza in merito all'adempimento dei propri compiti.

Per poter svolgere proficuamente le attività affidategli, il DPO si avvale del supporto del Servizio *Audit, Compliance, Risk Management* e *Privacy* e si confronta e coopera costantemente con la Direzione ICT della Società. Analogamente, ha un canale di dialogo preferenziale con il Servizio *Facility Management*, per quanto concerne i profili connessi alla gestione logistica ed alla sicurezza dei locali.

Il DPO, almeno una volta all'anno, relaziona il Consiglio di amministrazione in merito al livello di conformità al Regolamento, all'osservanza della normativa e delle politiche aziendali in materia di *data protection*, all'attuazione della Politica sulla protezione dei dati personali, agli esiti dell'attività di vigilanza svolta e formula suggerimenti per il miglioramento del sistema di *data protection*. In particolare, il DPO riporta:

- in maniera continuativa all'Amministratore Delegato, ogni qualvolta lo ritenga necessario e/o opportuno per l'attuazione degli obblighi previsti dal Regolamento, fornendo ogni informazione rilevante e/o utile per il corretto adempimento delle prescrizioni del Regolamento;
- con periodicità almeno annuale, mediante apposita relazione scritta, al Consiglio di Amministrazione, riepilogando le attività svolte, le eventuali richieste degli interessati pervenute, le eventuali richieste dell'autorità di controllo, e fornendo indicazioni e suggerimenti in merito agli interventi correttivi da adottare per rimuovere eventuali disallineamenti riscontrati.

Infine, nell'espletamento dell'attività, il DPO ha un canale di dialogo preferenziale con la Direzione ICT. In particolare, la Direzione ICT cura le politiche aziendali in materia di corretta gestione dei dati che transitano attraverso gli applicativi e/o le reti aziendali; definisce le misure generali per la protezione da accessi non autorizzati ed informazioni riservate (*User-id, password*, *screensaver* con *password*), per l'integrità e riservatezza delle informazioni (crittografia, anonimizzazione, ecc.), per possibili danneggiamenti (*antivirus*

e *firewall*), per la protezione da eventuali perdite di disponibilità di dati (*disaster recovery*, politiche di *back up*, etc.). La Direzione cura, inoltre, il procedimento di nomina e aggiornamento degli amministratori di sistema.

4.9 GLI AMMINISTRATORI DI SISTEMA

L'Amministratore di Sistema è definito nel Provvedimento del Garante del 27 novembre 2008 come "*una figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali*". La Società si è dotata di un regolamento *ad hoc* per gli amministratori di sistema allegato al presente MOP.

4.10 SERVIZIO AUDIT, COMPLIANCE, RISK MANAGEMENT E PRIVACY

Il Servizio *Audit, Compliance, Risk management e Privacy* verifica i Regolamenti aziendali in materia di *privacy*, supporta il Responsabile della protezione dei dati Personali nella definizione ed aggiornamento di un sistema formalizzato di gestione dei trattamenti di dati personali e nell'individuazione delle misure necessarie al fine di assicurare la conformità al Regolamento (UE) 2016/679 e al D.lgs. 196/2003 e ss.mm.ii.

5. POLICY DATA PROTECTION

La *Policy* (**Allegato 1**) si inserisce nel più ampio contesto del SGSI (Sistema di Gestione della Sicurezza delle Informazioni) implementato da Consap e delinea un sistema organico e strutturato di gestione degli aspetti concernenti i profili *privacy* (Sistema di gestione *privacy*) fornendo ai vari attori di tale sistema indicazioni chiare, sia sul piano tecnico/operativo e organizzativo sia circa le modalità di applicazione del Regolamento da parte della Società in qualità di Titolare o di Responsabile del trattamento, a seconda dei casi. La *Policy*, nello specifico:

- definisce, all'interno dell'organizzazione aziendale, ruoli, compiti e responsabilità degli organi / funzioni / soggetti coinvolti, a vari livelli e a diverso titolo, secondo le rispettive competenze e inquadramento;
- descrive le principali modalità operative stabilite dalla Società per effettuare il trattamento dei dati personali, fornendo indicazioni relative all'acquisizione, produzione, utilizzo e gestione, conservazione e trasmissione delle informazioni aziendali, con particolare attenzione a quelle di tipo elettronico che, per loro natura, risultano particolarmente critiche;
- individua le misure tecniche ed organizzative che Consap ha adottato e implementato per prevenire e/o ridurre i rischi di distruzione, perdita, accesso non autorizzato da parte di terzi, trattamento non consentito, modifica non autorizzata, furto, distruzione dei dati personali;
- disciplina l'adempimento dei principali obblighi previsti dalla normativa in materia di trattamento e protezione dei dati personali.

6. REGISTRO DEL TRATTAMENTO DEI DATI

La Società, in qualità sia di Titolare e sia di Responsabile del trattamento di dati personali, tiene un Registro delle attività di trattamento, in formato elettronico, all'interno del quale sono indicati:

a) nome e dati di contatto del Titolare del trattamento e del Responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) i trasferimenti di dati personali verso un paese terzo, ove applicabile;
f) i termini di cancellazione previsti per le diverse categorie di dati, ove possibile.

La Società assicura il costante aggiornamento del suddetto Registro e la sua messa a disposizione alle Autorità di Controllo. Al tal fine, la Consap S.p.A. attribuisce ai referenti *privacy*, con la collaborazione del DPO, la responsabilità in merito alla tenuta del Registro delle attività di trattamento. La rilevazione di un nuovo trattamento si verificherà nel momento in cui ricorrono, congiuntamente o disgiuntamente, le seguenti condizioni:

- si avviano trattamenti di dati personali su nuove categorie di interessati; su nuove tipologie di dati personali trattati; per nuove finalità;
- si avviano operazioni di trattamento che comportano la necessità di effettuare una nuova valutazione dei rischi o, in seconda battuta, una nuova valutazione d'impatto;
- mutano sostanzialmente gli attori del trattamento coinvolti, nei casi in cui ciò comporti la necessità di redigere una nuova valutazione dei rischi o, in seconda battuta, una nuova valutazione d'impatto.

In caso di nuovi trattamenti, ovvero di modifica ai trattamenti di dati personali già esistenti, il Responsabile interno competente in materia comunica tempestivamente al DPO le modifiche da apportare nel Registro dei trattamenti.
Nel registro delle attività di trattamento aggiornato alla pubblicazione del presente documento sono state individuate 21 attività di trattamento in qualità di Titolare del trattamento e 26 in qualità di Responsabile, per un totale di 47 attività di trattamento complessive.

7. RISK ASSESSMENT PRIVACY

Al fine di individuare le misure e le azioni necessarie per consentire l'adeguamento al Regolamento, la Società effettua una ricognizione del complessivo assetto organizzativo-gestionale e delle misure di sicurezza utilizzate per proteggere i dati personali nell'ambito dei processi di trattamento.

La metodologia adottata per svolgere detta attività è quella redatta da ENISA (Agenzia dell'Unione Europea per la *cybersicurezza*), per la valutazione del rischio di sicurezza, ai sensi dell'art. 32 GDPR, elaborato con il contributo del *Garante per la Privacy*.

L'approccio metodologico suggerito dall'ENISA si fonda su quattro fasi di seguito descritte:

- *Definizione dell'operazione di trattamento e del suo contesto*: individuazione delle peculiarità di ciascuna attività implicante il trattamento di dati personali e valutazione dei rischi connessi;
- *Comprensione e valutazione dell'impatto:* analisi dell'impatto che il trattamento può avere sui diritti e le libertà degli interessati in caso di violazione delle misure di sicurezza adottate;

- *Definizione di possibili minacce e valutazione della loro probabilità* (probabilità di occorrenza della minaccia): analisi delle minacce e delle probabilità che tali eventi negativi si verifichino;
- *Valutazione del rischio* (combinando la probabilità di accadimento della minaccia e l'impatto): ogni trattamento svolto è valutato combinando l'impatto sui diritti e le libertà degli interessati con la probabilità che le minacce si verifichino utilizzando una scala qualitativa composta da quattro livelli;
- *Analisi delle misure di sicurezza da implementare*: in base al risultato ottenuto dalla valutazione vengono individuate le misure volte alla riduzione del rischio.

Si è pertanto proceduto ad effettuare un'analisi dell'organizzazione delle attività di *business* e amministrative svolte dalla Società. All'esito dell'analisi, sono state identificate le principali aree di rischio relative alla *privacy*.
Il *driver* per la valutazione dei rischi (sicurezza informativa e sicurezza delle informazioni) è stato l'impatto potenziale di un incidente di sicurezza su diritti e libertà dell'interessato, valutato in combinazione con i tre aspetti che devono essere garantiti:

- **riservatezza**: l'impatto che una divulgazione non autorizzata dei dati potrebbe avere sull'individuo;
- **integrità:** l'impatto che un'alterazione non autorizzata dei dati personali potrebbe avere sull'individuo;
- **disponibilità:** l'impatto che una distruzione o perdita non autorizzata di dati personali potrebbe avere sull'individuo.

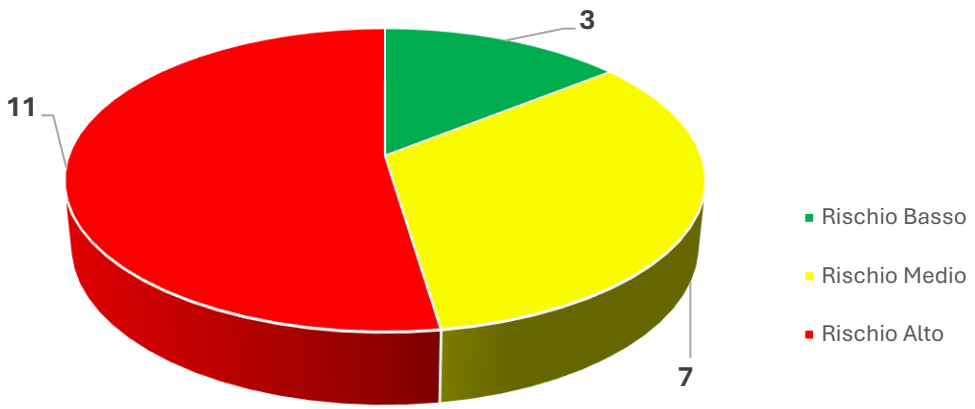
In virtù del procedimento sopra descritto sono stati individuati quattro livelli di valutazione del rischio per le attività di trattamento presenti nel registro dei trattamenti, di seguito rappresentati in dettaglio:

BASSO	Gli individui possono andare incontro a disagi minori che supereranno senza alcun problema
MEDIO	Gli individui possono andare incontro a significativi disagi che saranno in grado di superare nonostante alcune difficoltà
ALTO	Gli individui possono andare incontro a conseguenze significative che dovrebbero essere in grado di superare anche se con gravi difficoltà
MOLTO ALTO	Gli individui possono subire conseguenze significative o addiritura irreversibili che non sono in grado di superare

Di seguito sono illustrati graficamente i risultati dell'analisi dei rischi effettuata sui trattamenti:

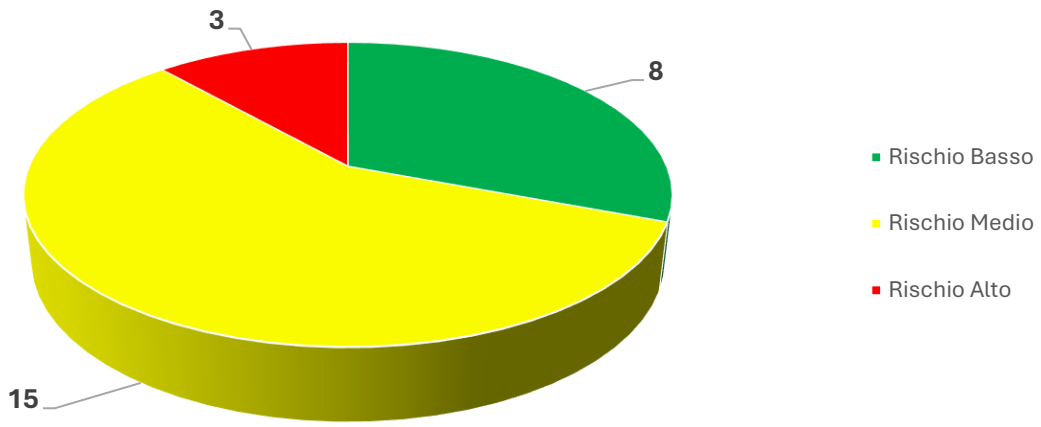
- Rischio trattamenti (Titolare) - Metodologia Valutazione dei rischi ENISA:

**N. trattamenti (Titolare) divisi per rischio*



- Rischio trattamenti (Responsabile) - Metodologia Valutazione dei rischi ENISA:

**N. trattamenti (Responsabile) divisi per rischio*



Al fine di predisporre un Modello organizzativo *privacy risk based* la Società si è servita di un apposito *tool* – GoPrivacy sviluppato da Sistemi H.S. S.p.A. – così da analizzare i rischi legati alla *privacy* delle attività di trattamento utilizzando la metodologia ENISA (European Union Agency For Cybersecurity).

Si riporta di seguito l'elenco delle attività di trattamento di cui la Società è Titolare, divisi in ordine di rischio crescente calcolato secondo la metodologia di valutazione dei rischi ENISA:

ID	Denominazione	Finalità	Interessati	Rischio
Segreteria societaria015	Segreteria societaria	Corretta gestione degli adempimenti societari (es. convocazione assemblee, convocazioni riunioni CdA e CS, verbalizzazione delle riunioni, comunicazioni, ecc.) e alle attività di supporto in favore degli organi sociali / di controllo in generale	Componenti degli organi sociali; Vertici aziendali	BASSO
Studi ed elaborazioni statistiche014	Studi ed elaborazioni statistiche - Direzione ICT	- valutazioni di Customer Satisfaction (anche a supporto del Servizio Comunicazione e Media Relation); - elaborazione delle informazioni su base macroaggregata a fini di condivisione con ISTAT e istituzioni pubbliche; - elaborazione delle informazioni su base macroaggregata per fornire rappresentazioni dei fenomeni di gestione delle attività affidate a Consap attraverso indici predeterminati.	Tutte le categorie di interessati i cui dati sono oggetto di trattamento da parte di Consap S.p.A. ai fini dell'erogazione dei servizi richiesti, secondo quanto previsto dalle previsioni normative e dalle Convenzioni / Disciplinari con le Pubbliche Amministrazioni di riferimento; Tutte le categorie di interessati i cui dati sono oggetto di trattamento nell'ambito dei servizi di HELP DESK	BASSO

ID	Denominazione	Finalità	Interessati	Rischio
Tesoreria e insurance013	Tesoreria e insurance - Direzione amministrazione, finanza e controllo	- gestione degli ordini di pagamento e alla effettuazione delle relative disposizioni (bonifico); - effettuazione di controlli sulla eventuale presenza di pendenze fiscali o di cartelle esattoriali, come previsto dalla vigente normativa; - Effettuazione dei pagamenti nell'ambito della gestione dei Fondi e degli altri servizi erogati da Consap; - Gestire tutti gli adempimenti operativi relativi alle provvidenze previste per il personale, quali coperture assicurative, sanitarie e infortunistiche.	Banche; Dipendenti; Imprese di assicurazione	BASSO
Amministrazione Gestioni Separate01	Amministrazione Gestioni Separate - Direzione amministrazione, finanza e controllo	Certificazione per il lavoro autonomo e determinano i versamenti fiscali delle gestioni separate; Formazione e messa in esecuzione del Ruolo (recupero del credito a mezzo dell'Agenzia delle Entrate - Riscossione S.p.A.)	Debitori (individuati a seconda dell'attività di volta in volta considerata rispetto al credito azionato)	MEDIO

ID	Denominazione	Finalità	Interessati	Rischio
Contabilità e bilancio012	Contabilità e bilancio - Direzione amministrazione, finanza e controllo	- registrazione delle fatture, alla consultazione dei relativi dati e al raffronto (anche con i relativi contratti / commesse di riferimento); - organizzare e coordinare l'organizzazione dei flussi documentali contabili; - gestire la predisposizione e l'invio, nonché gli eventuali successivi adempimenti richiesti dall'Agenzia delle Entrate, di istanze di rimborso a seguito di acquisto di crediti fiscali di Compagnie in l.c.a da parte del Fondo di Garanzia per le Vittime della Strada.	Agenzia delle Entrate; Compagnie in l.c.a.	MEDIO
Servizio rivalse020	Direzione Funzioni Assicurative - Servizio rivalse	- valutazione della sussistenza dei requisiti per procedere al recupero; - recupero coattivo delle somme liquidate per sinistri nei confronti dei non assicurati (NA); - definizione di un accordo transattivo con il soggetto non assicurato; - stralcio; - Analisi delle contestazioni ricevute dai non assicurati.	Danneggiati; Non assicurati; Testimoni	MEDIO

ID	Denominazione	Finalità	Interessati	Rischio
Progettazione gare	Direzione stazione appaltante - Progettazione gare (settore Sicurezza lavori)	- Supportare il RUP nella verifica della completezza e correttezza dei documenti di sicurezza forniti da imprese appaltatrici, subappaltatrici e lavoratori autonomi (DURC, idoneità, attestati formativi, nomine, DUVRI, ecc.); - supportare il RUP nell'effettuazione delle comunicazioni agli organi di controllo (es. ASL, Ispettorato del Lavoro, ecc.);	Asl; Fornitori	MEDIO

ID	Denominazione	Finalità	Interessati	Rischio
Facility Management008	Facility Management - Direzione risorse umane	- coordinare i fornitori esterni relativamente agli interventi di manutenzione ordinaria e straordinaria della Sede, compreso il controllo del funzionamento degli impianti e gli adempimenti amministrativi connessi previsti dalla legge; - assegnazione di stanze, mobilio e, in generale, alla gestione degli aspetti "fisici" delle postazioni di lavoro; - coordinare i servizi di facility management, quali reception e portierato, vigilanza notturna, pulizia, autisti Vertice Aziendale, telefonia, presidio global service, ristoro aziendale, distributori automatici; - gestire le procedure relative agli accessi e alla security aziendale, sia fisica che infrastrutturale, e le attività utili alla salvaguardia della business continuity, con riferimento agli impianti tecnologici a servizio della Sede.	Collaboratori; Consulenti esterni; Dipendenti; Fornitori; Stagisti	MEDIO

ID	Denominazione	Finalità	Interessati	Rischio
Gestione del sito internet istituzionale003	Gestione del sito internet istituzionale	- consentire di fruire del sito internet www.consap.it agli utenti, a garantire la sicurezza e il corretto funzionamento e ad effettuare analisi sull'utilizzo e sui contenuti a cui i visitatori accedono (anche per quanto riguarda la Sezione "Società Trasparente", in tal caso in conformità alle indicazioni dell'ANAC) e valutazioni di performance; - agevolare la gestione dei contatti da parte degli utenti, mediante un sistema dedicato di presentazione di richieste scritte (Contact Form).	Utenti che contattato Consap attraverso il Contact Form; Utenti che si registrano e accedono al Portale; Utenti internet; Visitatori della pagina web	MEDIO
Progetti innovativi e gestione documentale017	Progetti innovativi e gestione documentale - Direzione ICT	Gestione documentale ed elettronica dei documenti	Uffici interni	MEDIO
Affari giuridici, legislativi e segreteria tecnica018	Affari giuridici, legislativi e segreteria tecnica	- emettere o esaminare pareri legali su richiesta del Vertice Aziendale; - predisposizione o revisione di convenzioni, contratti, disciplinari ecc.;	Tutte le categorie di interessati i cui dati vengono trattati dalla Società nell'ambito e ai fini delle attività di business che essa svolge	ALTO

ID	Denominazione	Finalità	Interessati	Rischio
Affari legali005	Affari legali	- tutela, in ambito precontenzioso e/o contenzioso, dei diritti della Società con riferimento alle attività che essa svolge e ai rapporti che essa intrattiene; - tutela, in ambito precontenzioso e/o contenzioso, dei diritti della Società; - selezione e l'iscrizione di avvocati esterni all'Albo istituito dalla Società, per la sottoscrizione e gestione della Convenzione e per l'affidamento di incarichi professionali, sulla base della Convenzione stessa (con i conseguenti adempimenti di legge, anche in materia fiscale); - predisposizione o revisione di convenzioni, contratti, disciplinari ecc. - verifica della condizione socio-economica dei debitori.	Controparti contrattuali; Professionisti (avvocati); Tutte le categorie di interessati i cui dati vengono trattati dalla Società nell'ambito e ai fini delle attività di business che essa svolge	ALTO

Amministrazione del personale007	Amministrazione del personale - Direzione risorse umane	-(liquidazione e versamento delle competenze e di ogni altro emolumento spettanti al personale dipendente, anticipi e liquidazione a valere sul fondo T.F.R. aziendale al personale dipendente, comunicazioni con gli Enti competenti, pagamento di fondi di previdenza, ecc. - gestire la liquidazione e il versamento delle competenze ai componenti del Consiglio di Amministrazione, del Collegio Sindacale, dell'Organismo di Vigilanza, dei comitati del "Fondo di garanzia per le vittime della strada", del "Fondo di garanzia per le Vittime della Caccia", del "Fondo di rotazione per la solidarietà alle vittime dei reati di tipo mafioso, delle richieste estorsive, dell'usura e dei reati intenzionali violenti", del "Fondo di Garanzia per i mediatori di assicurazione e riassicurazione"; - gestire il trattamento economico delle trasferte del personale Consap; - gestire le richieste di concessione ai	Collaboratori; Componenti degli organi sociali; Dipendenti; Stagisti	ALTO

ID	Denominazione	Finalità	Interessati	Rischio
		dipendenti di prestiti personali e dei benefici in applicazione di quanto previsto nel C.I.A.; - gestire l'elaborazione, il controllo e la predisposizione del flusso per l'invio delle certificazioni uniche dei redditi da lavoro dipendente e assimilati erogati da Consap e dai Fondi.; Gestire gli adempimenti contabili relativi alle risorse in somministrazione lavoro; Gestire il Welfare aziendale		

ID	Denominazione	Finalità	Interessati	Rischio
Gare e contratti009	Gare e contratti - Stazione appaltante	- valutazione dei dati personali e alla gestione dei rapporti (es. con albo fornitori, ecc.); - selezione dei potenziali fornitori e all'effettuazione dei controlli previsti dalla normativa vigente, ai fini della eventuale contrattualizzazione; - elaborazione, revisione, gestione e conservazione (mediante archiviazione) della contrattualistica aziendale; - Trattamento dei dati personali di impiegati e collaboratori della Società finalizzato alla acquisizione, gestione e dismissione delle dotazioni aziendali assegnate al personale.	Componenti delle Commissioni di gara; Consulenti esterni; Dipendenti; Fornitori; Fornitori che intendono iscriversi / che sono iscritti all'Albo; Partecipanti alle gare / fornitori, anche potenziali; Stagisti	ALTO
Gestione della sicurezza fisica011	Gestione della sicurezza fisica: accessi alla sede e videosorveglianza	- Videosorveglianza finalizzata a garantire la sicurezza fisica della sede della Società; - Trattamento di dati personali di dipendenti, collaboratori e visitatori.	Componenti Organi sociali e di controllo; Consulenti esterni; Dipendenti; Passanti su strada (lungo il perimetro dell'ingresso principale); Visitatori	ALTO

Gestione risorse, organizzazione e relazioni industriali006	Gestione risorse, organizzazione e relazioni industriali - Direzione risorse umane	- Trattamento dei dati personali di persone fisiche coinvolte nel processo di ricerca e selezione del personale tramite candidature spontanee e ricerca diretta (LinkedIn, ecc.); - Trattamento dei dati personali di impiegati e collaboratori della Società finalizzato all'instaurazione e gestione del rapporto contrattuale, ai connessi adempimenti amministrativi e normativi, all'erogazione della formazione e all'adempimento degli obblighi in materia di salute e sicurezza nei luoghi di lavoro; - Trattamento di dati personali finalizzato alla valutazione periodica delle prestazioni del personale dipendente ai fini dell'eventuale assegnazione di premi di risultato secondo la Policy aziendale; - Gestione dei rapporti con le organizzazioni e rappresentanze sindacali, commissioni pari opportunità e mobbing; - Supporto al RSPP per gestione degli adempimenti in materia di tutela della salute e	Candidati; Collaboratori; Dipendenti; Organizzazioni sindacali; RSPP; Stagisti	ALTO

ID	Denominazione	Finalità	Interessati	Rischio
		sicurezza sui luoghi di lavoro.		
Monitoraggio contratti010	Monitoraggio contratti - Stazione appaltante	- Supporto RUP, DEC e DL in materia di fornitura e servizi; - Supporto all'attività di controllo della spese per l'esecuzione di lavori servizi e fornitori (tenuta della contabilità del contratto); - Apposizione del visto di conformità al pagamento delle fatture per le commesse Consap S.p.A.; - Monitoraggio sul rispetto dei tempi di consegna dei lavori; - Controllo sullo stato di avanzamento dei costi dei contratti e tracciabilità dei flussi finanziari (prevenzione antiriciclaggio).	Fornitori; Legali	ALTO

ID	Denominazione	Finalità	Interessati	Rischio
Portale Unico004	Portale Unico	- generazione dell'account personale e all'acquisizione da parte del sistema di dati da utilizzare per il successivo accesso ai servizi (mediante compilazione e invio di un apposito modulo di domanda); - consentire l'accesso dell'utente alla propria area personale; - autenticazione degli utenti al Portale Unico di Consap attraverso l'utilizzo delle credenziali SPID; - elaborazione del modulo di domanda / richiesta, mediante inserimento dei dati e informazioni richieste negli appositi campi del form di compilazione; - consentire la gestione delle funzionalità del Portale, a garantirne la sicurezza il corretto funzionamento e ad effettuare analisi sull'utilizzo da parte degli utenti e valutazioni di performance; - agevolare la richiesta telefonica di informazioni da parte degli utenti e il riscontro della Società.	Beneficiari; Richiedenti; Utenti; Utenti che si registrano e accedono al Portale; Visitatori della pagina web	ALTO

ID	Denominazione	Finalità	Interessati	Rischio
Servizio Audit, Compliance, Risk Management e *privacy*02	Servizio Audit, Compliance, Risk Management e *privacy*	- verifica sui processi aziendali (dati personali già oggetto di trattamento da parte delle Direzioni / altri Servizi); - conduzione delle attività di verifica in ambito Compliance; - adempimento degli obblighi normativi, nello svolgimento delle attività di Audit e nell'esecuzione delle attività disciplinate dalle Procedure per consentire l'esercizio dei diritti da parte degli interessati o per gestire eventuali violazioni di dati personali; - gestione delle richieste di esercizio dei diritti da parte degli interessati.	Tutte le tipologie di interessati i cui dati vengono trattati dalla Società	ALTO

ID	Denominazione	Finalità	Interessati	Rischio
Sistemi informativi016	Sistemi informativi - Direzione ICT	- monitoraggio delle attività IT; - profilazione degli utenti sui sistemi applicativi: creazione, abilitazione, amministrazione e disabilitazione / cancellazione degli account interni per l'operatività su sistemi e applicativi aziendali; - fornire assistenza agli utenti interni in ambito di Office Automation; - creazione, abilitazione, amministrazione e disabilitazione / cancellazione degli account interni di posta elettronica; - definire modelli decisionali aziendali basati su approccio di tipo “data-driven” .	Amministratori; Consulenti esterni; Dipendenti; Fornitori; Organi di controllo; Stagisti; Tutte le categorie di interessati di cui la Società tratta i dati personali	ALTO
Whistleblowing019	Whistleblowing	Gestione degli adempimenti in materia di whistleblowing di Consap Concessionaria dei Servizi Assicurativi Pubblici S.p.A.	Facilitatore; Persona coinvolta dalla segnalazione, c.d. “segnalato” (eventuale); Persone, oltre al segnalante, informate dei fatti oggetto di segnalazione (eventuali).; Segnalante	ALTO

Si riporta di seguit, seguendo la precedente metodologia, l’elenco delle attività di trattamento di cui la Società è Responsabile:

ID	Denominazione	Finalità	Interessati	Rischio
Bonus vista017	Bonus vista	- Accesso alla Piattaforma applicativa che consente agli esercenti di monitorare in autonomia lo stato delle fatture inviate; - Riscontro e alla liquidazione delle fatture elettroniche ricevute dagli esercenti per il rimborso dei voucher: registrazione, organizzazione, strutturazione, consultazione e raffronto, conservazione dei dati (comunicazione all'occorrenza, su richiesta); - Riscontro e alla liquidazione delle istanze di rimborso ricevute direttamente dai beneficiari per rimborso della spesa sostenuta: registrazione, organizzazione, strutturazione, consultazione e raffronto, conservazione dei dati (comunicazione all'occorrenza, su richiesta); - Liquidazione delle fatture agli esercenti; - Rimborso della somma già spesa; - Archiviazione della documentazione e alla conservazione delle basi di dati.	Beneficiari; Esercenti (e loro legali rappresentanti); Richiedenti; Richiedenti (Intestatari del c/c)	BASSO

ID	Denominazione	Finalità	Interessati	Rischio
Certificazioni navali008	Certificazioni navali	- ricezione delle domande per il rilascio della certificazione; - verifica della presenza della polizza assicurativa sottostante la certificazione; - rilascio della certificazione; - in caso di rilascio, invio del certificato al richiedente; - in caso di rigetto, comunicazione al richiedente delle motivazioni del rigetto; - in caso di sopravvenuta inefficacia della copertura assicurativa, contestazione da parte del soggetto che l'ha rilasciata, falsità delle attestazioni dichiarate o mancato pagamento dell'importo previsto per il rilascio del certificato, comunicazione della revoca all'Autorità che tiene il registro di iscrizione della nave; - archiviazione della documentazione; - ricezione delle domande per la pubblicazione del Certificato M.L.C.; - pubblicazione del Certificato sul registro elettronico.	Armatore; Proprietario della nave; Richiedenti	BASSO

ID	Denominazione	Finalità	Interessati	Rischio
Fondi Alluvionati & Fondo contributi in conto interesse L. 949/52 e Fondo Centrale di Garanzia L. 1068/19640015	Fondi Alluvionati (Fondo contributi L. 35/1995 e Fondo Centrale di Garanzia L. 1162/1966) & Fondo contributi in conto interesse L. 949/52 e Fondo Centrale di Garanzia L. 1068/1964	- acquisizione delle banche dati dai precedenti gestori dei Fondi (Mediocredito e Artigiancassa); - elaborazione dei conteggi per i contributi in conto interesse/valore della garanzia; - liquidazione dei contributi in conto interesse / escussione della garanzia; - recupero delle erogazioni nei casi di revoca del contributo/di revoca o inefficacia della garanzia; - conservazione, mediante archiviazione, della documentazione.	Beneficiari e loro familiari ed eredi	BASSO
Fondo Debiti P.A.014	Fondo di Garanzia per i debiti della Pubblica Amministrazione (c.d. “Fondo Debiti P.A.”)	- liquidazione degli importi dovuti ai creditori - archiviazione della documentazione	Creditori	BASSO
Fondo Dazieri012	Fondo di previdenza per il personale addetto alla gestione delle imposte di consumo (c.d. Fondo Dazieri)	- liquidazione degli importi dovuti ai beneficiari; - conservazione, mediante archiviazione, della documentazione.	Beneficiari (Dazieri) e aventi causa	BASSO
Fondo GACS004	Fondo GACS	Raccolta e lavorazione delle istanze di ammissione al fondo di garanzia e archivazione della documentazione	Banche; Legale rappresentante	BASSO

ID	Denominazione	Finalità	Interessati	Rischio
Fondo Juncker026	Fondo Juncker (Fondo di garanzia sulle operazioni finanziarie delle piattaforme di investimento promosse dall'istituto nazionale di promozione)	- Acquisire da CDP i dati analitici delle garanzie contenute nelle piattaforme di investimento; - effettuare gli accantonamenti disposti nel decreto di approvazione della piattaforma di investimento; - gestire gli adempimenti connessi all'escussione delle garanzie; - incassare le commissioni corrisposte da CDP quale corrispettivo per il rilascio della garanzia pubblica.	Beneficiari; Richiedenti	BASSO

ID	Denominazione	Finalità	Interessati	Rischio
Sisma imprese025	Sisma imprese	1. istruire le richieste di escussione trasmesse dagli istituti di credito; 2. procedere all'istruttoria delle richieste di escussione della garanzia dello Stato presentate dagli Istituti di credito direttamente al Ministero concedente ed il cui esame non sia stato ancora avviato ovvero completato; 3. disporre, all'esito dell'istruttoria, il pagamento delle escussioni sull'Iban indicato dagli istituti di credito; 4. trasmettere allo stesso Ministero tutti i dati, i documenti e le informazioni esplicative in possesso di Consap concernenti la posizione oggetto di contenzioso instaurato o minacciato, ciò anche al fine di consentire la costituzione in giudizio con il patrocinio dell'Avvocatura di Stato.	Imprese danneggiate che hanno richiesto la garanzia dello Stato	BASSO

ID	Denominazione	Finalità	Interessati	Rischio
"Carta della cultura Giovani", "Carta del merito" e "Carta del docente"016	"Carta della cultura Giovani", "Carta del merito" e "Carta del docente"	- accesso alla Piattaforma applicativa che consente agli esercenti di monitorare in autonomia lo stato delle fatture inviate; - riscontro e alla liquidazione delle fatture elettroniche ricevute dagli esercenti per il rimborso dei voucher: registrazione, organizzazione, strutturazione, consultazione e raffronto, conservazione dei dati (comunicazione all'occorrenza, su richiesta); - alla liquidazione delle fatture agli esercenti; - all'archiviazione della documentazione e alla conservazione delle basi di dati. Infine, trattamento di dati personali, attraverso cookie tecnici (di sessione), al solo scopo di migliorare le prestazioni del sito durante la navigazione, per ottimizzare l'esperienza dell'utente nell'accesso ai servizi richiesti.	ESERCENTI; Utenti che accedono al Portale e che chiedono assistenza	MEDIO

ID	Denominazione	Finalità	Interessati	Rischio
Buono Patente Autotrasporto019	Buono Patente Autotrasporto	- l' accesso alla Piattaforma applicativa che consente alle autoscuole di monitorare in autonomia lo stato delle fatture inviate; - migliorare le prestazioni del sito durante la navigazione, attraverso cookie tecnici (di sessione), per ottimizzare l'esperienza dell'utente nell'accesso ai servizi richiesti; - il riscontro e alla liquidazione delle fatture elettroniche ricevute dagli esercenti per il rimborso dei voucher: registrazione, organizzazione, strutturazione, consultazione e raffronto, conservazione dei dati (comunicazione all'occorrenza, su richiesta); - liquidazione delle fatture alle autoscuole; - archiviazione della documentazione e alla conservazione delle basi di dati.	Autoscuole (e loro legali rappresentanti); Utenti che accedono al Portale (1)	MEDIO

ID	Denominazione	Finalità	Interessati	Rischio
Centro di informazione italiano006	Centro di informazione italiano	Le finalità del trattamento sono le seguenti: - la fornitura di informazioni circa la copertura assicurativa del responsabile del sinistro; - l'apertura del fascicolo e all'avvio della lavorazione; - la gestione della richiesta relativa al sinistro, effettuando, per i responsabili italiani, le analisi necessarie attraverso la consultazione del Data Base delle coperture assicurative gestito dall'Ania (SITA) e, per i danneggiati italiani, le richieste ai Centri di informazione esteri; - l'invio di informativa circa le risultanze delle analisi condotte (estremi dell'assicurazione) al richiedente e al Centro di informazioni estero; - la conservazione, mediante archiviazione, della documentazione; - agevolare la richiesta di informazioni sull'utilizzo del Portale Unico da parte degli utenti e il riscontro della Società.	Bureau esteri; Danneggiati; Responsabile del sinistro; Richiedente (danneggiato o suo legale / soggetto delegato)	MEDIO

Fondo caccia024	Fondo di garanzia per le vittime della caccia	I dati personali, forniti direttamente dagli interessati (mediante la compilazione e invio del modulo di domanda e la produzione di documenti), oppure acquisiti dalle Imprese Designate[1], anche là dove si riferiscano a soggetti diversi dagli istanti (vedi i danneggianti o i testimoni), sono trattati per l'adempimento di un obbligo di legge (ai sensi dell'articolo 6, comma 1, lettera c) del Regolamento), per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (ai sensi dell'articolo 6, comma 1, lettera e) del Regolamento), nonché – ove si tratti di categorie di dati particolari – per motivi di interesse pubblico rilevante (ai sensi del combinato disposto degli articoli 9, comma 2, lettera g) del suddetto Regolamento e 2-sexies, comma 2, lett. m) del D. Lgs. 196/2003), esclusivamente al fine di svolgere le attività necessarie alla gestione amministrativa della pratica di liquidazione del sinistro, incluso l'avvio delle azioni esecutive volte al recupero delle somme elargite in favore dei danneggiati, secondo	Interessati che presentano domanda risarcitoria	MEDIO

ID	Denominazione	Finalità	Interessati	Rischio
		quanto previsto dalla normativa che disciplina l'operatività del Fondo in questione. La ricezione – direttamente da parte degli interessati, oppure mediante trasmissione ad opera delle Imprese Designate – e il trattamento dei dati personali sono indispensabili per svolgere le attività sopra indicate, previste dalla normativa di riferimento.		
Fondo di solidarietà per i mutui per l'acquisto della prima casa010	Fondo di solidarietà per i mutui per l'acquisto della prima casa	- raccolta e protocollazione delle domande di ammissione al Fondo; - raccolta delle istanze di ammissione al Fondo; - accettazione/rigetto della richiesta di ammissione al Fondo; - pagamento oneri finanziari, interessi e rate sospese; - contestazione e/o definizione di proposte transattive; - azione di regresso nei confronti del beneficiario e recupero coattivo; - conservazione, mediante archiviazione, della documentazione; - agevolare la richiesta telefonica di informazioni da parte degli utenti e il riscontro della Società.	Contitolari mutuo; Istanti; Utenti	MEDIO

FIR013	Fondo indennizzo risparmiatori (FIR)	registrazione degli utenti al Portale, alla generazione e manutenzione delle credenziali di autenticazione e alla gestione degli accessi degli utenti al Portale stesso; agevolare la richiesta di informazioni da parte degli utenti e il riscontro della Società; agevolare la richiesta telefonica di informazioni da parte degli utenti e il riscontro della Società; presentazione delle richieste di indennizzo e della documentazione di supporto da parte degli istanti; protocollazione e gestione del fascicolo elettronico della domanda, di eventuali integrazioni e dei documenti allegati in conformità delle linee guida previste da AgID; esame della documentazione ricevuta e alla verifica dei requisiti per la concessione dell'indennizzo; approvazione della richiesta di indennizzo, sulla base dell'esito dell'istruttoria, e di formulazione di una proposta di liquidazione sulla quale è chiamata ad esprimersi la Commissione tecnica; comunicazione della decisione della Commissione tecnica e delle modalità di pagamento; acquisire	Delegati; Familiari succeduti per atto inter vivos; Richiedenti; Risparmiatori richiedenti (consumatori, imprenditori individuali o agricoli, legali rappresentanti di microimprese o di organizzazione di volontariato e associazioni di promozione sociale); Successori mortis causa dei risparmiatori; Utenti; Utenti che si registrano e accedono alla Piattaforma; Visitatori della pagina web	MEDIO

ID	Denominazione	Finalità	Interessati	Rischio
		documentazione mancante ai fini del completamento dell'istruttoria della pratica successivamente alla disabilitazione dell'operatività esterna del Portale; pagamento degli indennizzi riconosciuti; l'effettuazione di analisi e l'elaborazione di report sulle attività di lavorazione delle pratiche (dati in forma pseudonimizzata); conservazione della documentazione relativa alle pratiche lavorate.		
Fondo nuovi nati021	Fondo nuovi nati	- gestione dell'escussione e alla verifica della sussistenza dei requisiti dell'istante (attività già svolta dalla Banca); - contestazione (ad es. false dichiarazioni) e/o definizione di proposte transattive; - azione di regresso nei confronti del beneficiario e recupero coattivo"; - archiviazione della documentazione.	Banche; Istanti	MEDIO

ID	Denominazione	Finalità	Interessati	Rischio
Fondo per gli acquirenti di beni immobili da costruire011	Fondo per gli acquirenti di beni immobili da costruire	-acquisizione e completamento delle istanze di ammissione al Fondo pregresse (Data entry); -gestione dell'archivio dati degli istanti ammessi al Fondo, le cui pratiche sono sospese fino alla re-immissione di quote nel Fondo stesso; - analisi ed istruttoria delle istanze, in caso di esito positivo è emessa una delibera di ammissione per accesso al Fondo; - pagamento degli interessati; - verifica periodica della sussistenza dei requisiti per l'utilizzo del Fondo; - alla contestazione (ad es. false dichiarazioni) e/o definizione di proposte transattive; - all'azione di regresso nei confronti del reo (costruttore) e recupero coattivo; - conservazione, mediante archiviazione, della documentazione; - agevolare la richiesta telefonica di informazioni da parte degli utenti e il riscontro della Società.	Imprenditori (fallito o in corso di procedura concorsuale-esecutiva); Istanti ed eredi	MEDIO

ID	Denominazione	Finalità	Interessati	Rischio
Fondo per lo studio020	Fondo per il credito ai giovani cd. "Fondo per lo studio"	- raccolta e protocollazione delle domande di ammissione al Fondo; - raccolta delle istanze di ammissione al rilascio della garanzia per accesso al credito; - accettazione/rigetto della richiesta di ammissione per erogazione del credito; - rilascio della garanzia per l'erogazione del credito previa comunicazione ricevuta dalla banca finanziatrice; - gestione dell'escussione ed alla verifica della sussistenza dei requisiti dell'istante (attività già svolta dalla Banca); - contestazione (ad es. false dichiarazioni) e/o definizione di proposte transattive; - azione di regresso nei confronti del beneficiario e recupero coattivo; - archiviazione della documentazione.	Istanti	MEDIO

Acquisto Autobus Alta Sostenibilità Ecologica018	Incentivo per acquisto Autobus Alta Sostenibilità Ecologica	- accesso alla Piattaforma applicativa che consente alle autoscuole di monitorare in autonomia lo stato delle fatture inviate; - attraverso cookie tecnici (di sessione), al solo scopo di migliorare le prestazioni del sito durante la navigazione, per ottimizzare l'esperienza dell'utente nell'accesso ai servizi richiesti; - riscontro e alla liquidazione delle fatture elettroniche ricevute dagli esercenti per il rimborso dei voucher: registrazione, organizzazione, strutturazione, consultazione e raffronto, conservazione dei dati (comunicazione all'occorrenza, su richiesta); - gestione degli adempimenti previsti rispetto al RNA; - pagamento del contributo deliberato dalla Commissione ministeriale in favore del richiedente (elaborazione del mandato di pagamento massivo ed eventuale gestione di singole posizioni anomale, richiedendo alle imprese informazioni o documenti); - archiviazione della documentazione e alla conservazione delle basi di dati.	Imprese (società di persone, ditte individuali); Legale rappresentante; Titolari di ditta individuale (intestatari del c/c); Utenti che accedono al Portale	MEDIO

ID	Denominazione	Finalità	Interessati	Rischio
Polizze dormienti023	Polizze dormienti	- ricezione delle richieste di rimborso e documentazione a supporto; - apertura della pratica nell'archivio informatico dei rapporti dormienti e comunicazione al richiedente della presa in carico; - esame della documentazione ricevuta; - verifica della pertinenza della domanda; - verifica dell'assenza della posizione in oggetto nell'archivio informatico; - verifica della presenza dell'importo richiesto con quanto indicato sugli elenchi dei rapporti dormienti; - comunicazione al richiedente dell'accoglimento / rigetto della domanda di rimborso; - pagamento dei rimborsi; - agevolare la richiesta di informazioni sull'utilizzo del Portale Unico da parte degli utenti e il riscontro della Società; - conservazione della documentazione relativa alle pratiche lavorate.	Richiedenti (anche liquidatori, eredi)	MEDIO

ID	Denominazione	Finalità	Interessati	Rischio
Rapporti dormienti022	Rapporti dormienti	- presentazione delle richieste di rimborso e documentazione a supporto; - apertura della pratica nell'archivio informatico dei rapporti dormienti e comunicazione al richiedente della presa in carico; - esame della documentazione ricevuta; - verifica della pertinenza della domanda; - verifica dell'assenza della posizione in oggetto nell'archivio informatico; - verifica della presenza dell'importo richiesto con quanto indicato sugli elenchi dei rapporti dormienti; - verifica a campione delle pratiche istruite da CONSAP prima dell'accoglimento; - comunicazione al richiedente dell'accoglimento / rigetto della domanda di rimborso; - pagamento dei rimborsi; - agevolare la richiesta di informazioni sull'utilizzo del Portale Unico da parte degli utenti e il riscontro della Società; - archiviazione della documentazione.	Persone defunte; Richiedenti (anche legali rappresentanti di società, liquidatori, eredi)	MEDIO

Ruolo dei periti assicurativi e fondo brokers005	Ruolo dei periti assicurativi e fondo brokers	Fondo Brokers. Trattamento di dati personali finalizzato esclusivamente al fine di svolgere le attività necessarie alla gestione della pratica risarcitoria e all'avvio delle azioni volte al recupero delle somme elargite in favore dei danneggiati, secondo quanto previsto dalla normativa che disciplina l'operatività del Fondo in questione.; Ruolo dei periti assicurativi. Trattamento di dati personali finalizzato a: - verificare l'effettivo svolgimento del periodo di tirocinio previsto dalla legge; - creazione dell'account personale e al successivo accesso all'area riservata per usufruire dei relativi servizi; - consentire la gestione delle funzionalità del Portale, a garantirne la sicurezza il corretto funzionamento e ad effettuare analisi statistiche sull'utilizzo e valutazioni di performance del sito; - iscrizione per la partecipazione all'esame di abilitazione da Periti Assicurativi RC Auto mediante presentazione della domanda attraverso le funzionalità dell'area riservata del Portale; - valutazione della prova di esame sostenuta dai candidati, anche attraverso strumenti	Candidati; Interessati che presentano domanda risarcitoria; Periti Assicurativi; Utenti che si registrano e accedono al Portale; Visitatori della pagina web	MEDIO

ID	Denominazione	Finalità	Interessati	Rischio
		automatizzati (prova risposta multipla); - informare i candidati dell'esito della prova di esame, mediante comunicazione resa disponibile nella loro area riservata del Portale applicativo; - ricezione ed esame della domanda di iscrizione e alla successiva pubblicazione dei dati del Perito Assicurativo nel Ruolo; - riscossione del contributo annuale, alla verifica del mantenimento dei requisiti previsti, all'irrogazione di sanzioni disciplinari, alla effettuazione di variazioni anagrafiche, ecc.; - cancellazione del Perito Assicurativo dal Ruolo; - verifica del possesso dei requisiti del perito per l'abilitazione come CTU; - recupero dei contributi annuali non versati dai Periti per l'iscrizione al Ruolo; - monitoraggio pagamento contributi d'iscrizione; - conservazione, mediante archiviazione, della documentazione (fascicolo personale del candidato e del Perito Assicurativo).		

Sistema di prevenzione del Furto d'Identità003	Sistema di prevenzione del Furto d'Identità	Le finalità del trattamento sono le seguenti: - acquisizione dei dati da sottoporre a verifica, alla trasmissione delle richieste di verifica all'Archivio Centrale informatizzato SCIPAFI e all'invio dei riscontri agli aderenti e ai soggetti autorizzati; - veicolazione delle richieste di interrogazione verso le banche dati di riferimento per la consultazione e alla ricezione del relativo riscontro semaforico da trasmettere agli aderenti e ai soggetti autorizzati, attraverso apposita infrastruttura informatica che gestisce l'interconnessione di reti; - stipula della convenzione con l'aderente e alla creazione, abilitazione e assegnazione, nonché variazione, delle utenze per i referenti individuati dagli aderenti; - consentire l'accesso al Portale web SCIPAFI, a monitorarne l'utilizzo da parte degli utenti abilitati degli aderenti e dei soggetti autorizzati e a controllarne il corretto funzionamento; - all'organizzazione delle riunioni (mediante convocazione dei partecipanti) e allo scambio di documenti e informazioni tra i componenti del	Persone fisiche che hanno subito o temono di aver subito frodi identitarie; Persone fisiche la cui identità è oggetto di verifica da parte degli aderenti e dei soggetti autorizzati, con riferimento alle attività previste dalla normativa; Referenti degli aderenti	MEDIO

ID	Denominazione	Finalità	Interessati	Rischio
		Gruppo di lavoro; - alla gestione delle richieste di assistenza di natura amministrativa e di carattere tecnico informatico pervenute dagli aderenti e dai soggetti autorizzati; - alla gestione delle richieste di assistenza riguardanti la necessità di approfondimenti su singoli riscontri, pervenute dagli aderenti e dai soggetti autorizzati; - alla ricezione di segnalazioni da parte dei soggetti che hanno subito o temono di aver subito frodi configuranti ipotesi di furto di identità; - all'attività di archiviazione della documentazione; - al monitoraggio del servizio offerto dal Sistema SCIPAFI in generale e dalle banche dati istituzionali collegate.		

ID	Denominazione	Finalità	Interessati	Rischio
Stanza di Compensazione007	Stanza di Compensazione	- Regolazione dei rapporti credito/debito tra le Compagnie aderenti alla CARD, provvedendo al rimborso della somma pagata al danneggiato a titolo di risarcimento; - Gestione dei rapporti con i contraenti delle polizze assicurative dei veicoli responsabili per consentire il rimborso del sinistro per evitare la maggiorazione del premio per l'evoluzione del Bonus/Malus; - Consentire la gestione delle funzionalità del Portale, a garantirne la sicurezza il corretto funzionamento e ad effettuare analisi statistiche sull'utiizzo e valutazioni di performance del sito; - Agevolare la richiesta telefonica di informazioni da parte degli utenti e il riscontro della Società.	Contraenti; Danneggiati; Imprese di assicurazione; Istanti; Utenti/Richiedenti	MEDIO

Fondo di Garanzia Mutui per la prima casa009	Fondo di Garanzia Mutui per la prima casa	-raccolta delle domande di ammissione al Fondo - raccolta delle istanze di ammissione al rilascio della garanzia per accesso al credito; -accettazione/rigetto della richiesta di ammissione per erogazione del credito; -rilascio della garanzia per l'erogazione del credito previa comunicazione ricevuta dalla banca finanziatrice; -gestione dell'escussione ed alla verifica della sussistenza dei requisiti dell'istante (attività già svolta dalla Banca); -contestazione (ad es. false dichiarazioni) e/o definizione di proposte transattive; -azione di regresso nei confronti del beneficiario e recupero coattivo; - conservazione, mediante archiviazione, della documentazione; - raccolta e protocollazione delle domande di ammissione al Fondo; -raccolta delle istanze di ammissione al Fondo; - accettazione/rigetto della richiesta di ammissione al Fondo; -pagamento oneri finanziari, interessi e rate sospese; -alla conservazione, mediante archiviazione, della documentazione; - richiesta telefonica di informazioni da parte	Banche; Istanti	ALTO

ID	Denominazione	Finalità	Interessati	Rischio
		degli utenti e il riscontro della Società.		

FGVS001	Fondo di Garanzia per le Vittime della Strada (C.F. 97114260587)	Finalità contrattuali e adempimento di obblighi legali; Finalità del trattamento è la ricezione delle richieste di risarcimento danni (in copia conoscenza) da parte dei danneggiati e/o legali dei danneggiati; Finalità del trattamento è la ricezione delle richieste di benestare per la liquidazione dei sinistri di importo superiore a 200.000 euro (importo parziale o totale del sinistro) da parte delle imprese designate; Trattamento dei dati personali finalizzato all'accettazione/rigetto della richiesta di liquidazione del sinistro da parte dell'impresa designata; Finalità del trattamento è la ricezione delle richieste di benestare per la liquidazione dei sinistri di importo superiore a 80.000 euro (importo parziale o totale del sinistro) da parte dei commissari liquidatori autorizzati e imprese cessionarie; Trattamento dei dati personali finalizzato all'accettazione/rigetto della richiesta di liquidazione del sinistro da parte dei commissari liquidatori autorizzati e imprese cessionarie; Trattamento di dati personali connesso ad indagini in caso di frode o sospetto di	Controparte; Danneggiati; Istanti; Testimoni; Utenti; Utenti che si registrano e accedono al Portale	ALTO

		frode, finalizzato alla costituzione in giudizio di CONSAP ; Trattamento dei dati personali finalizzato alla gestione dei reclami ricevuti da IVASS; Trattamento di dati personali finalizzato ad agevolare la richiesta telefonica di informazioni da parte degli utenti e il riscontro della Società.; Trattamento dati personali finalizzato al rimborso dei sinistri liquidati dalle imprese designate; Trattamento di dati personali finalizzato alla conduzione di verifiche di natura amministrativo contabile, presso le imprese designate, per la valutazione della corretta gestione dei sinistri liquidati; Trattamento di dati personali finalizzato alla conservazione, mediante archiviazione, dei documenti.; Trattamento di dati personali finalizzato: - alla valutazione della sussistenza dei requisiti per procedere al recupero - al recupero coattivo delle somme liquidate per sinistri nei confronti dei non assicurati (NA) - alla definizione di un accordo transattivo con il soggetto non assicurato - allo stralcio; Trattamento di dati personali		

ID	Denominazione	Finalità	Interessati	Rischio
		finalizzato all'analisi delle contestazioni ricevute dai non assicurati.		

Fondo vittime mafia, estorsione, usura, reati violenti e orfani per crimini domestici002	Fondo di rotazione per la solidarietà vittime tipo mafioso, richieste estorsive, usura, reati intenzionali violenti e orfani crimini domestici	Mafia e Reati Intenzionali Violenti, il trattamento di dati personali di persone fisiche è finalizzato: - alla raccolta dei dati della vittima di mafia ; - al versamento dell'elargizione deliberata dal Comitato solidarietà; - al versamento provvisionale (nel caso di circostanze particolari, ovvero prima della ricezione del Decreto commissariale); - all'azione di regresso nei confronti dei condannati per reati di mafia e nei confronti del danneggiato in caso di sentenza negativa; - concessione benefici mafia ed estorsione (compensazione); - all'archiviazione della documentazione.; Usura e estorsione: - alla raccolta dei dati della vittima di estorsione e usura; - alla stipula del contratto di mutuo; - alla concessione del mutuo e dell'elargizione in relazione agli importi deliberati dal Comitato di solidarietà e al versamento provvisionale; - al monitoraggio (per l'elargizione) dell'impiego dei fondi erogati in attività economiche, anche con l'ausilio di indagini pubbliche; - al recupero (per il mutuo) delle somme erogate	Creditori; Istanti ed eredi; Legali (Istanti e Rei); Rei	ALTO

ID	Denominazione	Finalità	Interessati	Rischio
		nei confronti dei beneficiari (ad es. in caso di utilizzo improprio dei fondi erogati o di decadenza dei requisiti per l'utilizzo del fondo) e all'azione di regresso nei confronti del reo e recupero coattivo; - all'archiviazione della documentazione; - all'apertura di un c/c dedicato intestato alla vittima, ma su cui può operare unicamente CONSAP e al versamento dell'elargizione deliberata dal Comitato solidarietà - alla gestione dei pagamenti definiti nel piano di investimento deliberato dal Comitato di solidarietà sulla base delle fatture ricevute.		

Si riporta di seguito la valutazione del **rischio Titolare** effettuata con la metodologia ENISA:

CONSAP SPA

Valutazione del rischio (Titolare)

ENISA

Ordinamento Report:

Denominazione Trattamento; Identificativo Trattamento

Valutazione del rischio (Titolare)	
Denominazione del Trattamento	
ID: Affari giuridici, legislativi e segreteria tecnica018	Affari giuridici, legislativi e segreteria tecnica
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Estrazione; Comunicazione mediante trasmissione; Registrazione; Raffronto; Organizzazione; Uso; Conservazione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Tutti i dati personali oggetto di trattamento da parte di Consap S.p.A.
Qual è la finalità di trattamento?	- emettere o esaminare pareri legali su richiesta del Vertice Aziendale; - predisposizione o revisione di convenzioni, contratti, disciplinari ecc.;
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Tutte le categorie di interessati i cui dati vengono trattati dalla Società nell'ambito e ai fini delle attività di business che essa svolge
Quali sono i destinatari dei dati personali?	N.A.
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	ALTO
IMPATTO SULL'INTEGRITÀ	MEDIO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	ALTO
Definizione delle possibili minacce e valutazione della loro probabilità	
A. RISORSE DI RETE E TECNICHE	
A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO

A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Affari giuridici, legislativi e segreteria tecnica

	Impatto		
Probabilità	**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
BASSO			✗
MEDIO			
ALTO			

Il livello di rischio del trattamento **Affari giuridici, legislativi e segreteria tecnica** è	ALTO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO ALTO

Valutazione del rischio (Titolare)

Denominazione del Trattamento

ID: Affari legali005	Affari legali

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Estrazione; Comunicazione mediante trasmissione; Registrazione; Organizzazione; Uso; Cancellazione; Conservazione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Altri dati: ogni eventuale altro dato o informazioni riferibile a persone fisiche contenuto nei documenti; Dati assicurativi; Dati bancari; Dati di contatto; Dati finanziari ed economici; Dati giudiziari; Dati identificativi; Dati previdenziali e assistenziali; Dati relativi a procedimenti giudiziari; Dati relativi al documento d'identità; Dati relativi alla qualifica professionale, alle mansioni e alla tipologia di lavoro svolto; Dati sanitari

Qual è la finalità di trattamento?	- tutela, in ambito precontenzioso e/o contenzioso, dei diritti della Società con riferimento alle attività che essa svolge e ai rapporti che essa intrattiene; - tutela, in ambito precontenzioso e/o contenzioso, dei diritti della Società; - selezione e l'iscrizione di avvocati esterni all'Albo istituito dalla Società, per la sottoscrizione e gestione della Convenzione e per l'affidamento di incarichi professionali, sulla base della Convenzione stessa (con i conseguenti adempimenti di legge, anche in materia fiscale); - predisposizione o revisione di convenzioni, contratti, disciplinari ecc. - verifica della condizione socio- economica dei debitori.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Controparti contrattuali; Professionisti (avvocati); Tutte le categorie di interessati i cui dati vengono trattati dalla Società nell'ambito e ai fini delle attività di business che essa svolge
Quali sono i destinatari dei dati personali?	
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	ALTO
IMPATTO SULL'INTEGRITÀ	MEDIO
IMPATTO SULLA DISPONIBILITÀ	MEDIO
Valutazione complessiva impatto (I)	ALTO
Definizione delle possibili minacce e valutazione della loro probabilità	
A. RISORSE DI RETE E TECNICHE	
A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO

A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO

D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Affari legali

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**			✗
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Affari legali** è	ALTO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO ALTO

Valutazione del rischio (Titolare)	
Denominazione del Trattamento	
ID: Amministrazione del personale007	Amministrazione del personale - Direzione risorse umane
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Estrazione; Comunicazione mediante trasmissione; Registrazione; Organizzazione; Uso; Cancellazione; Conservazione; Interconnessione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Dati bancari; Dati di contatto; Dati identificativi; dati identificativi di familiari del lavoratore per eventuali benefici (ad es. L. 104/92); Dati politici, religiosi o relativi all'affiliazione sindacale; Dati previdenziali e assistenziali; Dati relativi a ferie, permessi e congedi; Dati relativi all'affiliazione sindacale

Qual è la finalità di trattamento?	-(liquidazione e versamento delle competenze e di ogni altro emolumento spettanti al personale dipendente, anticipi e liquidazione a valere sul fondo T.F.R. aziendale al personale dipendente, comunicazioni con gli Enti competenti, pagamento di fondi di previdenza, ecc. - gestire la liquidazione e il versamento delle competenze ai componenti del Consiglio di Amministrazione, del Collegio Sindacale, dell'Organismo di Vigilanza, dei comitati del "Fondo di garanzia per le vittime della strada", del "Fondo di garanzia per le Vittime della Caccia", del "Fondo di rotazione per la solidarietà alle vittime dei reati di tipo mafioso, delle richieste estorsive, dell'usura e dei reati intenzionali violenti", del "Fondo di Garanzia per i mediatori di assicurazione e riassicurazione"; - gestire il trattamento economico delle trasferte del personale Consap; - gestire le richieste di concessione ai dipendenti di prestiti personali e dei benefici in applicazione di quanto previsto nel C.I.A.; - gestire l'elaborazione, il controllo e la predisposizione del flusso per l'invio delle certificazioni uniche dei redditi da lavoro dipendente e assimilati erogati da Consap e dai Fondi.; Gestire gli adempimenti contabili relativi alle risorse in somministrazione lavoro; Gestire il Welfare aziendale
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Collaboratori; Componenti degli organi sociali; Dipendenti; Stagisti
Quali sono i destinatari dei dati personali?	N.A.
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	ALTO
IMPATTO SULL'INTEGRITÀ	MEDIO
IMPATTO SULLA DISPONIBILITÀ	MEDIO
Valutazione complessiva impatto (I)	ALTO
Definizione delle possibili minacce e valutazione della loro probabilità	

A. RISORSE DI RETE E TECNICHE	
A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	SI
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO

C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	MEDIO	2
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Amministrazione del personale - Direzione risorse umane

	Impatto		
Probabilità	**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
BASSO			✗
MEDIO			
ALTO			

Il livello di rischio del trattamento **Amministrazione del personale - Direzione risorse umane** è	ALTO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO ALTO

Valutazione del rischio (Titolare)

Denominazione del Trattamento

ID: Amministrazione Gestioni Separate01	Amministrazione Gestioni Separate - Direzione amministrazione, finanza e controllo

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Registrazione; Organizzazione; Uso; Cancellazione; Conservazione
Quali sono le tipologie di dati personali trattati?	Dati di contatto; Dati finanziari ed economici; Dati identificativi
Qual è la finalità di trattamento?	Certificazione per il lavoro autonomo e determinano i versamenti fiscali delle gestioni separate; Formazione e messa in esecuzione del Ruolo (recupero del credito a mezzo dell'Agenzia delle Entrate - Riscossione S.p.A.)
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Debitori (individuati a seconda dell'attività di volta in volta considerata rispetto al credito azionato)

Quali sono i destinatari dei dati personali?	

Valutazione impatto potenziale

IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	MEDIO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO

B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	MEDIO	2

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Amministrazione Gestioni Separate - Direzione amministrazione, finanza e controllo

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**		X	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Amministrazione Gestioni Separate - Direzione amministrazione, finanza e controllo** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO

Valutazione del rischio (Titolare)	
Denominazione del Trattamento	
ID: Contabilità e bilancio012	Contabilità e bilancio - Direzione amministrazione, finanza e controllo
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Estrazione; Registrazione; Organizzazione; Adattamento / Modifica; Uso; Cancellazione; Conservazione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Dati bancari e/o relativi ai pagamenti; Dati di contatto; Dati finanziari ed economici
Qual è la finalità di trattamento?	- registrazione delle fatture, alla consultazione dei relativi dati e al raffronto (anche con i relativi contratti / commesse di riferimento); - organizzare e coordinare l'organizzazione dei flussi documentali contabili; - gestire la predisposizione e l'invio, nonché gli eventuali successivi adempimenti richiesti dall'Agenzia delle Entrate, di istanze di rimborso a seguito di acquisto di crediti fiscali di Compagnie in l.c.a da parte del Fondo di Garanzia per le Vittime della Strada.
Dove ha luogo il trattamento dei dati personali?	
Quali sono le categorie di interessati coinvolti?	Agenzia delle Entrate; Compagnie in l.c.a.
Quali sono i destinatari dei dati personali?	N.A.
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO

Definizione delle possibili minacce e valutazione della loro probabilità	
A. RISORSE DI RETE E TECNICHE	
A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO

C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Contabilità e bilancio - Direzione amministrazione, finanza e controllo

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**		✗	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Contabilità e bilancio - Direzione amministrazione, finanza e controllo** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO

Valutazione del rischio (Titolare)

Denominazione del Trattamento

ID: Servizio rivalse020	Direzione Funzioni Assicurative - Servizio rivalse

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Comunicazione mediante trasmissione; Registrazione; Organizzazione; Uso; Cancellazione; Conservazione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Dati bancari; Dati di contatto; Dati finanziari ed economici; Dati giudiziari; Dati identificativi; Dati relativi al documento d'identità; Dati relativi alla qualifica professionale, alle mansioni e alla tipologia di lavoro svolto
Qual è la finalità di trattamento?	- valutazione della sussistenza dei requisiti per procedere al recupero; - recupero coattivo delle somme liquidate per sinistri nei confronti dei non assicurati (NA); - definizione di un accordo transattivo con il soggetto non assicurato; - stralcio; - Analisi delle contestazioni ricevute dai non assicurati.

Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Danneggiati; Non assicurati; Testimoni
Quali sono i destinatari dei dati personali?	N.A.

Valutazione impatto potenziale

IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO

B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Direzione Funzioni Assicurative - Servizio rivalse

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**		✗	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Direzione Funzioni Assicurative - Servizio rivalse** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO

Valutazione del rischio (Titolare)	
Denominazione del Trattamento	
ID: Progettazione gare	Direzione stazione appaltante - Progettazione gare (settore Sicurezza lavori)
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Registrazione; Organizzazione; Uso; Conservazione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Dati di contatto; Dati previdenziali e assistenziali
Qual è la finalità di trattamento?	- Supportare il RUP nella verifica della completezza e correttezza dei documenti di sicurezza forniti da imprese appaltatrici, subappaltatrici e lavoratori autonomi (DURC, idoneità, attestati formativi, nomine, DUVRI, ecc.); - supportare il RUP nell'effettuazione delle comunicazioni agli organi di controllo (es. ASL, Ispettorato del Lavoro, ecc.);
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Asl; Fornitori
Quali sono i destinatari dei dati personali?	N.A.
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO
Definizione delle possibili minacce e valutazione della loro probabilità	
A. RISORSE DI RETE E TECNICHE	

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO

C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Direzione stazione appaltante - Progettazione gare (settore Sicurezza lavori)

	Impatto			
Probabilità		**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
	BASSO		X	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Direzione stazione appaltante - Progettazione gare (settore Sicurezza lavori)** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO

Valutazione del rischio (Titolare)

Denominazione del Trattamento

ID: Facility Management008	Facility Management - Direzione risorse umane

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Estrazione; Registrazione; Organizzazione; Uso; Cancellazione; Conservazione; Distruzione
Quali sono le tipologie di dati personali trattati?	Dati di contatto; Dati identificativi; Dati relativi al documento d'identità; Dati relativi al percorso di studi, alla qualifica professionale, all'inquadramento contrattuale, alle mansioni e alla tipologia di lavoro svolto

Qual è la finalità di trattamento?	- coordinare i fornitori esterni relativamente agli interventi di manutenzione ordinaria e straordinaria della Sede, compreso il controllo del funzionamento degli impianti e gli adempimenti amministrativi connessi previsti dalla legge; - assegnazione di stanze, mobilio e, in generale, alla gestione degli aspetti "fisici" delle postazioni di lavoro; - coordinare i servizi di facility management, quali reception e portierato, vigilanza notturna, pulizia, autisti Vertice Aziendale, telefonia, presidio global service, ristoro aziendale, distributori automatici; - gestire le procedure relative agli accessi e alla security aziendale, sia fisica che infrastrutturale, e le attività utili alla salvaguardia della business continuity, con riferimento agli impianti tecnologici a servizio della Sede.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Collaboratori; Consulenti esterni; Dipendenti; Fornitori; Stagisti
Quali sono i destinatari dei dati personali?	N.A.

Valutazione impatto potenziale

IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO

A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO

D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	NO
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Facility Management - Direzione risorse umane

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**		✗	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Facility Management - Direzione risorse umane** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO

Valutazione del rischio (Titolare)

Denominazione del Trattamento

ID: Gare e contratti009	Gare e contratti - Stazione appaltante

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Estrazione; Registrazione; Raffronto; Organizzazione; Uso; Cancellazione; Conservazione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Dati di contatto; Dati finanziari ed economici; Dati giudiziari; Dati identificativi; Dati previdenziali; Dati relativi all'assenza di incompatibilità e/o conflitti di interesse per i componenti delle Commissioni di gara; Dati relativi alla qualifica professionale, alle mansioni e alla tipologia di lavoro svolto; Dato personale relativo a condanne penali e reati

Qual è la finalità di trattamento?	- valutazione dei dati personali e alla gestione dei rapporti (es. con albo fornitori, ecc.); - selezione dei potenziali fornitori e all'effettuazione dei controlli previsti dalla normativa vigente, ai fini della eventuale contrattualizzazione; - elaborazione, revisione, gestione e conservazione (mediante archiviazione) della contrattualistica aziendale; - Trattamento dei dati personali di impiegati e collaboratori della Società finalizzato alla acquisizione, gestione e dismissione delle dotazioni aziendali assegnate al personale.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Componenti delle Commissioni di gara; Consulenti esterni; Dipendenti; Fornitori; Fornitori che intendono iscriversi / che sono iscritti all'Albo; Partecipanti alle gare / fornitori, anche potenziali; Stagisti
Quali sono i destinatari dei dati personali?	N.A.

Valutazione impatto potenziale

IMPATTO SULLA RISERVATEZZA	ALTO
IMPATTO SULL'INTEGRITÀ	MEDIO
IMPATTO SULLA DISPONIBILITÀ	MEDIO
Valutazione complessiva impatto (I)	ALTO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO

A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI

D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Gare e contratti - Stazione appaltante

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**			X
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Gare e contratti - Stazione appaltante** è	ALTO

è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO ALTO

Valutazione del rischio (Titolare)	
Denominazione del Trattamento	
ID: Gestione del sito internet istituzionale003	Gestione del sito internet istituzionale
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Estrazione; Registrazione; Organizzazione; Cancellazione; Conservazione; Interconnessione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Altri dati: eventuali dati personali forniti spontaneamente dagli utenti in relazione alla richiesta formulata; Dati di contatto; Dati identificativi; Eventuali identificativi numerici o alfanumerici (numero di pratica)
Qual è la finalità di trattamento?	- consentire l'usufruizione del sito internet www.consap.it agli utenti, a garantire la sicurezza e il corretto funzionamento e ad effettuare analisi sull'utilizzo e sui contenuti a cui i visitatori accedono (anche per quanto riguarda la Sezione "Società Trasparente", in tal caso in conformità alle indicazioni dell'ANAC) e valutazioni di performance; - agevolare la gestione dei contatti da parte degli utenti, mediante un sistema dedicato di presentazione di richieste scritte (Contact Form).
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Utenti che contattato Consap attraverso il Contact Form; Utenti che si registrano e accedono al Portale; Utenti internet; Visitatori della pagina web
Quali sono i destinatari dei dati personali?	
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MEDIO

IMPATTO SULL'INTEGRITÀ	MEDIO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	SI
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	SI
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	MEDIO	2
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Gestione del sito internet istituzionale

	Impatto			
Probabilità		**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
	BASSO		✗	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Gestione del sito internet istituzionale** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO

Valutazione del rischio (Titolare)

Denominazione del Trattamento

ID: Gestione della sicurezza fisica011	Gestione della sicurezza fisica: accessi alla sede e videosorveglianza

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Estrazione; Comunicazione mediante trasmissione; Registrazione; Diffusione / Messa a disposizione; Uso; Cancellazione; Conservazione; Distruzione
Quali sono le tipologie di dati personali trattati?	Dati di immagine; Dati identificativi; Dati relativi al documento d'identità

Qual è la finalità di trattamento?	- Videosorveglianza finalizzata a garantire la sicurezza fisica della sede della Società; - Trattamento di dati personali di dipendenti, collaboratori e visitatori.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Componenti Organi sociali e di controllo; Consulenti esterni; Dipendenti; Passanti su strada (lungo il perimetro dell'ingresso principale); Visitatori
Quali sono i destinatari dei dati personali?	N.A.

Valutazione impatto potenziale

IMPATTO SULLA RISERVATEZZA	ALTO
IMPATTO SULL'INTEGRITÀ	MEDIO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	ALTO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO

D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Gestione della sicurezza fisica: accessi alla sede e videosorveglianza

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**			✗
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Gestione della sicurezza fisica: accessi alla sede e videosorveglianza** è	ALTO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO ALTO

Valutazione del rischio (Titolare)	
Denominazione del Trattamento	
ID: Gestione risorse, organizzazione e relazioni industriali006	Gestione risorse, organizzazione e relazioni industriali - Direzione risorse umane
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Estrazione; Comunicazione mediante trasmissione; Registrazione; Organizzazione; Uso; Cancellazione; Conservazione; Interconnessione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Dati bancari; Dati di contatto; Dati finanziari, economici e patrimoniali (tasse universitarie e ammontare del finanziamento richiesto); Dati giudiziari; Dati identificativi; dati identificativi di familiari del lavoratore per eventuali benefici (ad es. L. 104/92); Dati politici, religiosi o relativi all'affiliazione sindacale; Dati relativi a ferie, permessi e congedi; Dati relativi a procedimenti disciplinari / sanzioni; Dati relativi al percorso di studi, alla qualifica professionale, all'inquadramento contrattuale, alle mansioni e alla tipologia di lavoro svolto; Dati relativi all'orientamento sessuale; Dati relativi alla carriera e all'apprendimento professionale; Dati relativi alla qualifica professionale, alle mansioni e alla tipologia di lavoro svolto; Dati sanitari (appartenenza a categorie protette); Dato personale relativo a condanne penali e reati
Qual è la finalità di trattamento?	- Trattamento dei dati personali di persone fisiche coinvolte nel processo di ricerca e selezione del personale tramite candidature spontanee e ricerca diretta (LinkedIn, ecc.); - Trattamento dei dati personali di impiegati e collaboratori della Società finalizzato all'instaurazione e gestione del rapporto contrattuale, ai connessi adempimenti amministrativi e normativi, all'erogazione della formazione e all'adempimento degli obblighi in materia di salute e sicurezza nei luoghi di lavoro; - Trattamento di dati personali finalizzato alla valutazione periodica delle prestazioni del personale dipendente ai fini dell'eventuale assegnazione di premi di risultato secondo la Policy aziendale; - Gestione dei rapporti con le organizzazioni e rappresentanze sindacali, commissioni pari opportunità e mobbing; - Supporto al RSPP per gestione degli adempimenti in materia di tutela della salute e sicurezza sui luoghi di lavoro.
Dove ha luogo il trattamento dei dati personali?	

Quali sono le categorie di interessati coinvolti?	Candidati; Collaboratori; Dipendenti; Organizzazioni sindacali; RSPP; Stagisti
Quali sono i destinatari dei dati personali?	N.A.

Valutazione impatto potenziale

IMPATTO SULLA RISERVATEZZA	ALTO
IMPATTO SULL'INTEGRITÀ	MEDIO
IMPATTO SULLA DISPONIBILITÀ	MEDIO
Valutazione complessiva impatto (I)	ALTO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	SI
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO

B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio

A. RISORSE DI RETE E TECNICHE	MEDIO	2
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Gestione risorse, organizzazione e relazioni industriali - Direzione risorse umane

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**			✗
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Gestione risorse, organizzazione e relazioni industriali - Direzione risorse umane** è	ALTO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO ALTO

Valutazione del rischio (Titolare)

Denominazione del Trattamento

ID: Monitoraggio contratti010	Monitoraggio contratti - Stazione appaltante

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Estrazione; Registrazione; Organizzazione; Uso; Cancellazione; Conservazione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Dati bancari e/o relativi ai pagamenti; Dati identificativi; Dati previdenziali
Qual è la finalità di trattamento?	- Supporto RUP, DEC e DL in materia di fornitura e servizi; - Supporto all'attività di controllo della spese per l'esecuzione di lavori servizi e fornitori (tenuta della contabilità del contratto); - Apposizione del visto di conformità al pagamento delle fatture per le commesse Consap S.p.A.; - Monitoraggio sul rispetto dei tempi di consegna dei lavori; - Controllo sullo stato di avanzamento dei costi dei contratti e tracciabilità dei flussi finanziari (prevenzione antiriciclaggio).
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Fornitori; Legali
Quali sono i destinatari dei dati personali?	N.A.

Valutazione impatto potenziale

IMPATTO SULLA RISERVATEZZA	ALTO
IMPATTO SULL'INTEGRITÀ	MEDIO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	ALTO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO

A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Monitoraggio contratti - Stazione appaltante

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**			✗
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Monitoraggio contratti - Stazione appaltante** è	ALTO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO / ALTO

Valutazione del rischio (Titolare)

Denominazione del Trattamento

ID: Portale Unico004	Portale Unico

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Estrazione; Comunicazione mediante trasmissione; Registrazione; Uso; Cancellazione; Conservazione; Interconnessione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Dati di contatto; Dati identificativi; File di log associati al servizio che traccia il flusso di autenticazione tra il Portale Unico e gli Identity Provider AgID. Il log contiene la richiesta di autenticazione e la relativa risposta, comprendendo i dati personali degli utenti.; Identificativi numerici o alfanumerici (Credenziali di autenticazione: user id e password); Tutti i dati trattati, rispettivamente, dai servizi che utilizzano il Portale Unico ai fini della ricezione delle domande / richieste e della gestione delle pratiche

Qual è la finalità di trattamento?	- generazione dell'account personale e all'acquisizione da parte del sistema di dati da utilizzare per il successivo accesso ai servizi (mediante compilazione e invio di un apposito modulo di domanda); - consentire l'accesso dell'utente alla propria area personale; - autenticazione degli utenti al Portale Unico di Consap attraverso l'utilizzo delle credenziali SPID; - elaborazione del modulo di domanda / richiesta, mediante inserimento dei dati e informazioni richieste negli appositi campi del form di compilazione; - consentire la gestione delle funzionalità del Portale, a garantirne la sicurezza il corretto funzionamento e ad effettuare analisi sull'utilizzo da parte degli utenti e valutazioni di performance; - agevolare la richiesta telefonica di informazioni da parte degli utenti e il riscontro della Società.
Dove ha luogo il trattamento dei dati personali?	
Quali sono le categorie di interessati coinvolti?	Beneficiari; Richiedenti; Utenti; Utenti che si registrano e accedono al Portale; Visitatori della pagina web
Quali sono i destinatari dei dati personali?	

Valutazione impatto potenziale

IMPATTO SULLA RISERVATEZZA	ALTO
IMPATTO SULL'INTEGRITÀ	MEDIO
IMPATTO SULLA DISPONIBILITÀ	MEDIO
Valutazione complessiva impatto (I)	ALTO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	SI
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI

A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	SI
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO

D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	MEDIO	2
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Portale Unico

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**			✗
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Portale Unico** è	ALTO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO ALTO

Valutazione del rischio (Titolare)	
Denominazione del Trattamento	
ID: Progetti innovativi e gestione documentale017	Progetti innovativi e gestione documentale - Direzione ICT
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Estrazione; Comunicazione mediante trasmissione; Registrazione; Diffusione / Messa a disposizione; Organizzazione; Uso; Cancellazione; Conservazione; Distruzione; Strutturazione; Limitazione
Quali sono le tipologie di dati personali trattati?	Tutte le categorie di dati oggetto di attività di trattamento da parte della Società
Qual è la finalità di trattamento?	Gestione documentale ed elettronica dei documenti
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Uffici interni
Quali sono i destinatari dei dati personali?	N.A.
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	MEDIO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO
Definizione delle possibili minacce e valutazione della loro probabilità	
A. RISORSE DI RETE E TECNICHE	

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO

C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Progetti innovativi e gestione documentale - Direzione ICT

	Impatto			
Probabilità		**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
	BASSO		X	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Progetti innovativi e gestione documentale - Direzione ICT** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO

Valutazione del rischio (Titolare)

Denominazione del Trattamento

ID: Segreteria societaria015	Segreteria societaria

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Estrazione; Uso; Cancellazione; Conservazione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Dati di contatto; Dati e informazioni rilevanti ai fini delle attività proprie degli Organi amministrativi e di controllo, nonché dei Vertici aziendali, contenuti in delibere e atti ufficiali.; Dati identificativi
Qual è la finalità di trattamento?	Corretta gestione degli adempimenti societari (es. convocazione assemblee, convocazioni riunioni CdA e CS, verbalizzazione delle riunioni, comunicazioni, ecc.) e alle attività di supporto in favore degli organi sociali / di controllo in generale
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Componenti degli organi sociali; Vertici aziendali

Quali sono i destinatari dei dati personali?	N.A.
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	BASSO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	BASSO
Definizione delle possibili minacce e valutazione della loro probabilità	
A. RISORSE DI RETE E TECNICHE	
A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO

B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio

A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Segreteria societaria

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**	X		
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Segreteria societaria** è	BASSO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO

Valutazione del rischio (Titolare)	
Denominazione del Trattamento	
ID: Servizio Audit, Compliance, Risk Management e privacy02	Servizio Audit, Compliance, Risk Management e privacy
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Estrazione; Comunicazione mediante trasmissione; Registrazione; Raffronto; Organizzazione; Uso; Cancellazione; Conservazione; Interconnessione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Tutte le categorie di dati oggetto di attività di trattamento da parte della Società
Qual è la finalità di trattamento?	- verifica sui processi aziendali (dati personali già oggetto di trattamento da parte delle Direzioni / altri Servizi); - conduzione delle attività di verifica in ambito Compliance; - adempimento degli obblighi normativi, nello svolgimento delle attività di Audit e nell'esecuzione delle attività disciplinate dalle Procedure per consentire l'esercizio dei diritti da parte degli interessati o per gestire eventuali violazioni di dati personali; - gestione delle richieste di esercizio dei diritti da parte degli interessati.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Tutte le tipologie di interessati i cui dati vengono trattati dalla Società
Quali sono i destinatari dei dati personali?	
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	ALTO
IMPATTO SULL'INTEGRITÀ	MEDIO
IMPATTO SULLA DISPONIBILITÀ	BASSO

Valutazione complessiva impatto (I)	ALTO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO

C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1

Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Servizio Audit, Compliance, Risk Management e privacy

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**			✗
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Servizio Audit, Compliance, Risk Management e privacy** è	ALTO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO ALTO

Valutazione del rischio (Titolare)	
Denominazione del Trattamento	
ID: Sistemi informativi016	Sistemi informativi - Direzione ICT
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Estrazione; Registrazione; Raffronto; Diffusione / Messa a disposizione; Organizzazione; Uso; Cancellazione; Conservazione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Dati di contatto aziendali; Dati identificativi; Dati relativi alla qualifica professionale, alle mansioni e alla tipologia di lavoro svolto; Identificativi numerici o alfanumerici (Credenziali di autenticazione: user id e password); Log di sistema e dati di traffico; Tutti i dati personali presenti nei Databases aziendali
Qual è la finalità di trattamento?	- monitoraggio delle attività IT; - profilazione degli utenti sui sistemi applicativi: creazione, abilitazione, amministrazione e disabilitazione / cancellazione degli account interni per l'operatività su sistemi e applicativi aziendali; - fornire assistenza agli utenti interni in ambito di Office Automation; - creazione, abilitazione, amministrazione e disabilitazione / cancellazione degli account interni di posta elettronica; - definire modelli decisionali aziendali basati su approccio di tipo "data-driven" .
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Amministratori; Consulenti esterni; Dipendenti; Fornitori; Organi di controllo; Stagisti; Tutte le categorie di interessati di cui la Società tratta i dati personali
Quali sono i destinatari dei dati personali?	N.A.
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	ALTO
IMPATTO SULL'INTEGRITÀ	MEDIO

IMPATTO SULLA DISPONIBILITÀ	MEDIO
Valutazione complessiva impatto (I)	ALTO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO

C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1

Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Sistemi informativi - Direzione ICT

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**			✗
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Sistemi informativi - Direzione ICT** è	ALTO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO ALTO

Valutazione del rischio (Titolare)

Denominazione del Trattamento

ID: Studi ed elaborazioni statistiche014	Studi ed elaborazioni statistiche - Direzione ICT

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Estrazione; Organizzazione; Cancellazione; Conservazione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Tutti i dati personali oggetto di trattamento da parte di Consap S.p.A.; Tutti i dati personali trattati per consentire l'evasione delle richieste di informazioni da parte degli utenti tramite HELP DESK

Qual è la finalità di trattamento?	- valutazioni di Customer Satisfaction (anche a supporto del Servizio Comunicazione e Media Relation); - elaborazione delle informazioni su base macroaggregata a fini di condivisione con ISTAT e istituzioni pubbliche; - elaborazione delle informazioni su base macroaggregata per fornire rappresentazioni dei fenomeni di gestione delle attività affidate a Consap attraverso indici predeterminati.
Dove ha luogo il trattamento dei dati personali?	
Quali sono le categorie di interessati coinvolti?	Tutte le categorie di interessati i cui dati sono oggetto di trattamento da parte di Consap S.p.A. ai fini dell'erogazione dei servizi richiesti, secondo quanto previsto dalle previsioni normative e dalle Convenzioni / Disciplinari con le Pubbliche Amministrazioni di riferimento; Tutte le categorie di interessati i cui dati sono oggetto di trattamento nell'ambito dei servizi di HELP DESK
Quali sono i destinatari dei dati personali?	N.A.

Valutazione impatto potenziale

IMPATTO SULLA RISERVATEZZA	BASSO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	BASSO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO

A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO

D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Studi ed elaborazioni statistiche - Direzione ICT

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**	✗		
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Studi ed elaborazioni statistiche - Direzione ICT** è	BASSO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO

Valutazione del rischio (Titolare)

Denominazione del Trattamento

ID: Tesoreria e insurance013	Tesoreria e insurance - Direzione amministrazione, finanza e controllo

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Consultazione; Estrazione; Comunicazione mediante trasmissione; Registrazione; Organizzazione; Uso; Cancellazione; Conservazione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Dati bancari e/o relativi ai pagamenti; Dati di contatto; Dati finanziari ed economici; Dati identificativi

Qual è la finalità di trattamento?	- gestione degli ordini di pagamento e alla effettuazione delle relative disposizioni (bonifico); - effettuazione di controlli sulla eventuale presenza di pendenze fiscali o di cartelle esattoriali, come previsto dalla vigente normativa; - Effettuazione dei pagamenti nell'ambito della gestione dei Fondi e degli altri servizi erogati da Consap; - Gestire tutti gli adempimenti operativi relativi alle provvidenze previste per il personale, quali coperture assicurative, sanitarie e infortunistiche.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Banche; Dipendenti; Imprese di assicurazione
Quali sono i destinatari dei dati personali?	N.A.

Valutazione impatto potenziale

IMPATTO SULLA RISERVATEZZA	BASSO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	BASSO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO

A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI

D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Tesoreria e insurance - Direzione amministrazione, finanza e controllo

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**	✗		
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Tesoreria e insurance - Direzione amministrazione, finanza e controllo** è	BASSO

è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO

Valutazione del rischio (Titolare)	
Denominazione del Trattamento	
ID: Whistleblowing019	Whistleblowing
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Uso; Cancellazione; Conservazione
Quali sono le tipologie di dati personali trattati?	Dati di contatto (del segnalante); Dati identificativi (del segnalante e del segnalato); Dati relativi alla qualifica professionale (ruolo o funzione aziendale del segnalante e del segnalato); Log di sistema
Qual è la finalità di trattamento?	Gestione degli adempimenti in materia di whistleblowing di Consap Concessionaria dei Servizi Assicurativi Pubblici S.p.A.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Facilitatore; Persona coinvolta dalla segnalazione, c.d. "segnalato" (eventuale); Persone, oltre al segnalante, informate dei fatti oggetto di segnalazione (eventuali).; Segnalante
Quali sono i destinatari dei dati personali?	N.A.
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MOLTO ALTO
IMPATTO SULL'INTEGRITÀ	MOLTO ALTO
IMPATTO SULLA DISPONIBILITÀ	MOLTO ALTO
Valutazione complessiva impatto (I)	MOLTO ALTO

Definizione delle possibili minacce e valutazione della loro probabilità	
A. RISORSE DI RETE E TECNICHE	
A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO

C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Whistleblowing

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**			X
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Whistleblowing** è	ALTO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO ALTO

Si riporta di seguito la valutazione del **rischio Responsabile** effettuata con la metodologia ENISA:

CONSAP SPA

Valutazione del rischio (Responsabile)

ENISA

Ordinamento Report:

Denominazione Trattamento; Identificativo Trattamento

Valutazione del rischio (Responsabile)	
Denominazione del Trattamento	
ID: "Carta della cultura Giovani", "Carta del merito" e "Carta del docente"016	"Carta della cultura Giovani", "Carta del merito" e "Carta del docente"
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Consultazione; Estrazione; Uso; Comunicazione mediante trasmissione; Cancellazione; Distruzione
Quali sono le tipologie di dati personali trattati?	Dati bancari; Dati di contatto; Dati identificativi; Dati identificativi numerici e alfanumerici (password); Dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di internet tra i quali, a titolo esemplificativo, indirizzi IP o nomi a dominio dei computer utilizzati dagli utenti che si connettono alla pagina, indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente; Log di sistema e dati di traffico
Qual è la finalità di trattamento?	- accesso alla Piattaforma applicativa che consente agli esercenti di monitorare in autonomia lo stato delle fatture inviate; - riscontro e alla liquidazione delle fatture elettroniche ricevute dagli esercenti per il rimborso dei voucher: registrazione, organizzazione, strutturazione, consultazione e raffronto, conservazione dei dati (comunicazione all'occorrenza, su richiesta); - alla liquidazione delle fatture agli esercenti; - all'archiviazione della documentazione e alla conservazione delle basi di dati. Infine, trattamento di dati personali, attraverso cookie tecnici (di sessione), al solo scopo di migliorare le prestazioni del sito durante la navigazione, per ottimizzare l'esperienza dell'utente nell'accesso ai servizi richiesti.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	ESERCENTI; Utenti che accedono al Portale e che chiedono assistenza
Quali sono i destinatari dei dati personali?	N.A.

Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	SI
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO

B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio

A. RISORSE DI RETE E TECNICHE	MEDIO	2
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento "Carta della cultura Giovani", "Carta del merito" e "Carta del docente"

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**		X	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **"Carta della cultura Giovani", "Carta del merito" e "Carta del docente"** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO

Valutazione del rischio (Responsabile)	
Denominazione del Trattamento	
ID: Bonus vista017	Bonus vista
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Consultazione; Estrazione; Uso; Cancellazione; Distruzione
Quali sono le tipologie di dati personali trattati?	Altri dati: codice di richiesta; Dati bancari; Dati di contatto; Dati identificativi (del richiedente e del beneficiario, se diverso); Log di sistema e dati di traffico
Qual è la finalità di trattamento?	- Accesso alla Piattaforma applicativa che consente agli esercenti di monitorare in autonomia lo stato delle fatture inviate; - Riscontro e alla liquidazione delle fatture elettroniche ricevute dagli esercenti per il rimborso dei voucher: registrazione, organizzazione, strutturazione, consultazione e raffronto, conservazione dei dati (comunicazione all'occorrenza, su richiesta); - Riscontro e alla liquidazione delle istanze di rimborso ricevute direttamente dai beneficiari per rimborso della spesa sostenuta: registrazione, organizzazione, strutturazione, consultazione e raffronto, conservazione dei dati (comunicazione all'occorrenza, su richiesta); - Liquidazione delle fatture agli esercenti; - Rimborso della somma già spesa; - Archiviazione della documentazione e alla conservazione delle basi di dati.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Beneficiari; Esercenti (e loro legali rappresentanti); Richiedenti; Richiedenti (Intestatari del c/c)
Quali sono i destinatari dei dati personali?	
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	BASSO
IMPATTO SULL'INTEGRITÀ	BASSO

IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	BASSO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	SI
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO

C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	MEDIO	2
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1

Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Bonus vista

	Impatto			
Probabilità		**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
	BASSO	✗		
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Bonus vista** è	BASSO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO

Valutazione del rischio (Responsabile)

Denominazione del Trattamento

ID: Buono Patente Autotrasporto019	Buono Patente Autotrasporto

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Consultazione; Uso; Cancellazione; Distruzione

Quali sono le tipologie di dati personali trattati?	Dati di contatto; Dati identificativi; Dati identificativi numerici e alfanumerici (password); Dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di internet tra i quali, a titolo esemplificativo, indirizzi IP o nomi a dominio dei computer utilizzati dagli utenti che si connettono alla pagina, indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente; Log di sistema e dati di traffico
Qual è la finalità di trattamento?	- l' accesso alla Piattaforma applicativa che consente alle autoscuole di monitorare in autonomia lo stato delle fatture inviate; - migliorare le prestazioni del sito durante la navigazione, attraverso cookie tecnici (di sessione), per ottimizzare l'esperienza dell'utente nell'accesso ai servizi richiesti; - il riscontro e alla liquidazione delle fatture elettroniche ricevute dagli esercenti per il rimborso dei voucher: registrazione, organizzazione, strutturazione, consultazione e raffronto, conservazione dei dati (comunicazione all'occorrenza, su richiesta); - liquidazione delle fatture alle autoscuole; - archiviazione della documentazione e alla conservazione delle basi di dati.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Autoscuole (e loro legali rappresentanti); Utenti che accedono al Portale (1)
Quali sono i destinatari dei dati personali?	
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO

Definizione delle possibili minacce e valutazione della loro probabilità	
A. RISORSE DI RETE E TECNICHE	
A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	SI
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO

C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	NO
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	MEDIO	2
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Buono Patente Autotrasporto

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**		✗	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Buono Patente Autotrasporto** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO

Valutazione del rischio (Responsabile)

Denominazione del Trattamento

ID: Centro di informazione italiano006	Centro di informazione italiano

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Consultazione; Uso; Interconnessione; Comunicazione mediante trasmissione; Diffusione / Messa a disposizione; Cancellazione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Altri dati: impresa di assicurazione (del responsabile del sinistro) e nazione di accadimento del sinistro, data e ora; Dati di contatto del richiedente; Dati identificativi (del richiedente e del danneggiato); Targa auto del veicolo responsabile del sinistro

Qual è la finalità di trattamento?	Le finalità del trattamento sono le seguenti: - la fornitura di informazioni circa la copertura assicurativa del responsabile del sinistro; - l'apertura del fascicolo e all'avvio della lavorazione; - la gestione della richiesta relativa al sinistro, effettuando, per i responsabili italiani, le analisi necessarie attraverso la consultazione del Data Base delle coperture assicurative gestito dall'Ania (SITA) e, per i danneggiati italiani, le richieste ai Centri di informazione esteri; - l'invio di informativa circa le risultanze delle analisi condotte (estremi dell'assicurazione) al richiedente e al Centro di informazioni estero; - la conservazione, mediante archiviazione, della documentazione; - agevolare la richiesta di informazioni sull'utilizzo del Portale Unico da parte degli utenti e il riscontro della Società.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Bureau esteri; Danneggiati; Responsabile del sinistro; Richiedente (danneggiato o suo legale / soggetto delegato)
Quali sono i destinatari dei dati personali?	

Valutazione impatto potenziale

IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	MEDIO
IMPATTO SULLA DISPONIBILITÀ	MEDIO
Valutazione complessiva impatto (I)	MEDIO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO

A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Centro di informazione italiano

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**		✗	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Centro di informazione italiano** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO

Valutazione del rischio (Responsabile)

Denominazione del Trattamento

ID: Certificazioni navali008	Certificazioni navali

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Consultazione; Uso; Cancellazione; Distruzione
Quali sono le tipologie di dati personali trattati?	Dati di contatto; Dati identificativi

Qual è la finalità di trattamento?	- ricezione delle domande per il rilascio della certificazione; - verifica della presenza della polizza assicurativa sottostante la certificazione; - rilascio della certificazione; - in caso di rilascio, invio del certificato al richiedente; - in caso di rigetto, comunicazione al richiedente delle motivazioni del rigetto; - in caso di sopravvenuta inefficacia della copertura assicurativa, contestazione da parte del soggetto che l'ha rilasciata, falsità delle attestazioni dichiarate o mancato pagamento dell'importo previsto per il rilascio del certificato, comunicazione della revoca all'Autorità che tiene il registro di iscrizione della nave; - archiviazione della documentazione; - ricezione delle domande per la pubblicazione del Certificato M.L.C.; - pubblicazione del Certificato sul registro elettronico.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Armatore; Proprietario della nave; Richiedenti
Quali sono i destinatari dei dati personali?	N.A.
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	BASSO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	BASSO
Definizione delle possibili minacce e valutazione della loro probabilità	
A. RISORSE DI RETE E TECNICHE	
A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO

A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Certificazioni navali

	Impatto			
Probabilità		**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
	BASSO	X		
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Certificazioni navali** è	BASSO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO

Valutazione del rischio (Responsabile)	
Denominazione del Trattamento	
ID: Fondi Alluvionati & Fondo contributi in conto interesse L. 949/52 e Fondo Centrale di Garanzia L. 1068/19640015	Fondi Alluvionati (Fondo contributi L. 35/1995 e Fondo Centrale di Garanzia L. 1162/1966) & Fondo contributi in conto interesse L. 949/52 e Fondo Centrale di Garanzia L. 1068/1964
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Uso; Comunicazione mediante trasmissione; Cancellazione; Distruzione
Quali sono le tipologie di dati personali trattati?	Dati bancari; Dati di contatto; Dati finanziari ed economici; Dati identificativi; Dati relativi al documento d'identità
Qual è la finalità di trattamento?	- acquisizione delle banche dati dai precedenti gestori dei Fondi (Mediocredito e Artigiancassa); - elaborazione dei conteggi per i contributi in conto interesse/valore della garanzia; - liquidazione dei contributi in conto interesse / escussione della garanzia; - recupero delle erogazioni nei casi di revoca del contributo/di revoca o inefficacia della garanzia; - conservazione, mediante archiviazione, della documentazione.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Beneficiari e loro familiari ed eredi
Quali sono i destinatari dei dati personali?	N.A.
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	BASSO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO

Valutazione complessiva impatto (I)	BASSO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO

C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1

Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Fondi Alluvionati (Fondo contributi L. 35/1995 e Fondo Centrale di Garanzia L. 1162/1966) & Fondo contributi in conto interesse L. 949/52 e Fondo Centrale di Garanzia L. 1068/1964

	Impatto			
Probabilità		**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
	BASSO	X		
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Fondi Alluvionati (Fondo contributi L. 35/1995 e Fondo Centrale di Garanzia L. 1162/1966) & Fondo contributi in conto interesse L. 949/52 e Fondo Centrale di Garanzia L. 1068/1964** è	BASSO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO

Valutazione del rischio (Responsabile)

Denominazione del Trattamento

ID: Fondo di Garanzia Mutui per la prima casa009	Fondo di Garanzia Mutui per la prima casa

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Uso; Comunicazione mediante trasmissione; Cancellazione; Distruzione

Quali sono le tipologie di dati personali trattati?	Dati di contatto; Dati identificativi; Dati relativi al documento d'identità; Dati relativi all'orientamento sessuale (unioni civili e altre forme di convivenza tra persone dello stesso sesso); Dati relativi alla qualifica professionale, alle mansioni e alla tipologia di lavoro svolto
Qual è la finalità di trattamento?	-raccolta delle domande di ammissione al Fondo - raccolta delle istanze di ammissione al rilascio della garanzia per accesso al credito; -accettazione/rigetto della richiesta di ammissione per erogazione del credito; -rilascio della garanzia per l'erogazione del credito previa comunicazione ricevuta dalla banca finanziatrice; -gestione dell'escussione ed alla verifica della sussistenza dei requisiti dell'istante (attività già svolta dalla Banca); -contestazione (ad es. false dichiarazioni) e/o definizione di proposte transattive; -azione di regresso nei confronti del beneficiario e recupero coattivo; -conservazione, mediante archiviazione, della documentazione; -raccolta e protocollazione delle domande di ammissione al Fondo; -raccolta delle istanze di ammissione al Fondo; -accettazione/rigetto della richiesta di ammissione al Fondo; -pagamento oneri finanziari, interessi e rate sospese; -alla conservazione, mediante archiviazione, della documentazione; -richiesta telefonica di informazioni da parte degli utenti e il riscontro della Società.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Banche; Istanti
Quali sono i destinatari dei dati personali?	N.A.
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	ALTO
IMPATTO SULL'INTEGRITÀ	MEDIO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	ALTO

Definizione delle possibili minacce e valutazione della loro probabilità	
A. RISORSE DI RETE E TECNICHE	
A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO

C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	SI
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	MEDIO	2
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	MEDIO	2
Probabilità complessiva di occorrenza minaccia (P)	MEDIO	**Punteggio:** 6

Valutazione del livello di rischio del trattamento Fondo di Garanzia Mutui per la prima casa

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**			
	MEDIO			✗
	ALTO			

Il livello di rischio del trattamento **Fondo di Garanzia Mutui per la prima casa** è	ALTO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO / ALTO

Valutazione del rischio (Responsabile)

Denominazione del Trattamento

ID: Fondo Debiti P.A.014	Fondo di Garanzia per i debiti della Pubblica Amministrazione (c.d. "Fondo Debiti P.A.")

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Uso; Cancellazione; Distruzione
Quali sono le tipologie di dati personali trattati?	Dati identificativi
Qual è la finalità di trattamento?	- liquidazione degli importi dovuti ai creditori - archiviazione della documentazione
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Creditori
Quali sono i destinatari dei dati personali?	N.A.

Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	BASSO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	BASSO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO

B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Fondo di Garanzia per i debiti della Pubblica Amministrazione (c.d. "Fondo Debiti P.A.")

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**	✗		
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Fondo di Garanzia per i debiti della Pubblica Amministrazione (c.d. "Fondo Debiti P.A.")** è	BASSO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO

Valutazione del rischio (Responsabile)	
Denominazione del Trattamento	
ID: Fondo caccia024	Fondo di garanzia per le vittime della caccia
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Consultazione; Estrazione; Uso; Cancellazione; Distruzione
Quali sono le tipologie di dati personali trattati?	Dati finanziari ed economici; Dati identificativi; Dati relativi alla qualifica professionale, alle mansioni e alla tipologia di lavoro svolto; Dati sanitari
Qual è la finalità di trattamento?	I dati personali, forniti direttamente dagli interessati (mediante la compilazione e invio del modulo di domanda e la produzione di documenti), oppure acquisiti dalle Imprese Designate[1], anche là dove si riferiscano a soggetti diversi dagli istanti (vedi i danneggianti o i testimoni), sono trattati per l'adempimento di un obbligo di legge (ai sensi dell'articolo 6, comma 1, lettera c) del Regolamento), per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (ai sensi dell'articolo 6, comma 1, lettera e) del Regolamento), nonché – ove si tratti di categorie di dati particolari – per motivi di interesse pubblico rilevante (ai sensi del combinato disposto degli articoli 9, comma 2, lettera g) del suddetto Regolamento e 2-sexies, comma 2, lett. m) del D. Lgs. 196/2003), esclusivamente al fine di svolgere le attività necessarie alla gestione amministrativa della pratica di liquidazione del sinistro, incluso l'avvio delle azioni esecutive volte al recupero delle somme elargite in favore dei danneggiati, secondo quanto previsto dalla normativa che disciplina l'operatività del Fondo in questione. La ricezione – direttamente da parte degli interessati, oppure mediante trasmissione ad opera delle Imprese Designate – e il trattamento dei dati personali sono indispensabili per svolgere le attività sopra indicate, previste dalla normativa di riferimento.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Interessati che presentano domanda risarcitoria
Quali sono i destinatari dei dati personali?	

Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO

B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Fondo di garanzia per le vittime della caccia

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**		X	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Fondo di garanzia per le vittime della caccia** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO

Valutazione del rischio (Responsabile)

Denominazione del Trattamento

ID: FGVS001	Fondo di Garanzia per le Vittime della Strada (C.F. 97114260587)

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Consultazione; Adattamento / Modifica; Estrazione; Raffronto; Uso; Comunicazione mediante trasmissione; Cancellazione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Dati assicurativi; Dati di contatto; Dati finanziari ed economici; Dati giudiziari; Dati identificativi; Dati relativi al documento d'identità; Dati sanitari
Qual è la finalità di trattamento?	Finalità contrattuali e adempimento di obblighi legali; Finalità del trattamento è la ricezione delle richieste di risarcimento danni (in copia conoscenza) da parte dei danneggiati e/o legali dei danneggiati; Finalità del trattamento è la ricezione delle richieste di benestare per la liquidazione dei sinistri di importo superiore a 200.000 euro (importo parziale o totale del sinistro) da parte delle imprese designate; Trattamento dei dati personali finalizzato all'accettazione/rigetto della richiesta di liquidazione del sinistro da parte dell'impresa designata; Finalità del trattamento è la ricezione delle richieste di benestare per la liquidazione dei sinistri di importo superiore a 80.000 euro (importo parziale o totale del sinistro) da parte dei commissari liquidatori autorizzati e imprese cessionarie; Trattamento dei dati personali finalizzato all'accettazione/rigetto della richiesta di liquidazione del sinistro da parte dei commissari liquidatori autorizzati e imprese cessionarie; Trattamento di dati personali connesso ad indagini in caso di frode o sospetto di frode, finalizzato alla costituzione in giudizio di CONSAP ; Trattamento dei dati personali finalizzato alla gestione dei reclami ricevuti da IVASS; Trattamento di dati personali finalizzato ad agevolare la richiesta telefonica di informazioni da parte degli utenti e il riscontro della Società.; Trattamento dati personali finalizzato al rimborso dei sinistri liquidati dalle imprese designate; Trattamento di dati personali finalizzato alla conduzione di verifiche di natura amministrativo contabile, presso le imprese designate, per la valutazione della corretta gestione dei sinistri liquidati; Trattamento di dati personali finalizzato alla conservazione, mediante archiviazione, dei documenti.; Trattamento di dati personali finalizzato: - alla valutazione della sussistenza dei requisiti per procedere al recupero - al recupero coattivo delle somme liquidate per sinistri nei confronti dei non assicurati (NA) - alla definizione di un accordo transattivo con il soggetto non assicurato - allo stralcio; Trattamento di dati personali finalizzato all'analisi delle contestazioni ricevute dai non assicurati.
Dove ha luogo il trattamento dei dati personali?	Roma

Quali sono le categorie di interessati coinvolti?	Controparte; Danneggiati; Istanti; Testimoni; Utenti; Utenti che si registrano e accedono al Portale
Quali sono i destinatari dei dati personali?	Organismi esteri (in caso di sinistro passivo)

Valutazione impatto potenziale

IMPATTO SULLA RISERVATEZZA	ALTO
IMPATTO SULL'INTEGRITÀ	MEDIO
IMPATTO SULLA DISPONIBILITÀ	MEDIO
Valutazione complessiva impatto (I)	ALTO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO

B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	SI
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	MEDIO	2
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Fondo di Garanzia per le Vittime della Strada (C.F. 97114260587)

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**			✗
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Fondo di Garanzia per le Vittime della Strada (C.F. 97114260587)** è	ALTO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO / ALTO

Valutazione del rischio (Responsabile)	
Denominazione del Trattamento	
ID: Fondo Dazieri012	Fondo di previdenza per il personale addetto alla gestione delle imposte di consumo (c.d. Fondo Dazieri)
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Uso; Cancellazione; Distruzione
Quali sono le tipologie di dati personali trattati?	Dati bancari; Dati di contatto; Dati finanziari ed economici; Dati identificativi; Dati relativi a persone defunte (eventuale); Dati relativi al documento d'identità; Dati relativi alla qualifica professionale, alle mansioni e alla tipologia di lavoro svolto
Qual è la finalità di trattamento?	- liquidazione degli importi dovuti ai beneficiari; - conservazione, mediante archiviazione, della documentazione.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Beneficiari (Dazieri) e aventi causa
Quali sono i destinatari dei dati personali?	N.A.
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	BASSO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	BASSO
Definizione delle possibili minacce e valutazione della loro probabilità	

A. RISORSE DI RETE E TECNICHE	
A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO

C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Fondo di previdenza per il personale addetto alla gestione delle imposte di consumo (c.d. Fondo Dazieri)

	Impatto			
Probabilità		**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
	BASSO	X		
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Fondo di previdenza per il personale addetto alla gestione delle imposte di consumo (c.d. Fondo Dazieri)** è	BASSO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO

Valutazione del rischio (Responsabile)

Denominazione del Trattamento

ID: Fondo vittime mafia, estorsione, usura, reati violenti e orfani per crimini domestici002	Fondo di rotazione per la solidarietà vittime tipo mafioso, richieste estorsive, usura, reati intenzionali violenti e orfani crimini domestici

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Consultazione; Uso; Comunicazione mediante trasmissione; Cancellazione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Categorie particolari di dati personali; Dati personali; Dato personale relativo a condanne penali e reati

Qual è la finalità di trattamento?	Mafia e Reati Intenzionali Violenti, il trattamento di dati personali di persone fisiche è finalizzato: - alla raccolta dei dati della vittima di mafia ; - al versamento dell'elargizione deliberata dal Comitato solidarietà; - al versamento provvisionale (nel caso di circostanze particolari, ovvero prima della ricezione del Decreto commissariale); - all'azione di regresso nei confronti dei condannati per reati di mafia e nei confronti del danneggiato in caso di sentenza negativa; - concessione benefici mafia ed estorsione (compensazione); - all'archiviazione della documentazione.; Usura e estorsione: - alla raccolta dei dati della vittima di estorsione e usura; - alla stipula del contratto di mutuo; - alla concessione del mutuo e dell'elargizione in relazione agli importi deliberati dal Comitato di solidarietà e al versamento provvisionale; - al monitoraggio (per l'elargizione) dell'impiego dei fondi erogati in attività economiche, anche con l'ausilio di indagini pubbliche; - al recupero (per il mutuo) delle somme erogate nei confronti dei beneficiari (ad es. in caso di utilizzo improprio dei fondi erogati o di decadenza dei requisiti per l'utilizzo del fondo) e all'azione di regresso nei confronti del reo e recupero coattivo; - all'archiviazione della documentazione; - all'apertura di un c/c dedicato intestato alla vittima, ma su cui può operare unicamente CONSAP e al versamento dell'elargizione deliberata dal Comitato solidarietà - alla gestione dei pagamenti definiti nel piano di investimento deliberato dal Comitato di solidarietà sulla base delle fatture ricevute.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Creditori; Istanti ed eredi; Legali (Istanti e Rei); Rei
Quali sono i destinatari dei dati personali?	
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MOLTO ALTO
IMPATTO SULL'INTEGRITÀ	ALTO
IMPATTO SULLA DISPONIBILITÀ	ALTO
Valutazione complessiva impatto (I)	MOLTO ALTO

Definizione delle possibili minacce e valutazione della loro probabilità	
A. RISORSE DI RETE E TECNICHE	
A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO

C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	SI

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	MEDIO	2
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Fondo di rotazione per la solidarietà vittime tipo mafioso, richieste estorsive, usura, reati intenzionali violenti e orfani crimini domestici

	Impatto		
Probabilità	**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
BASSO			✗
MEDIO			
ALTO			

Il livello di rischio del trattamento **Fondo di rotazione per la solidarietà vittime tipo mafioso, richieste estorsive, usura, reati intenzionali violenti e orfani crimini domestici** è	ALTO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO / ALTO

Valutazione del rischio (Responsabile)

Denominazione del Trattamento

ID: Fondo di solidarietà per i mutui per l'acquisto della prima casa010	Fondo di solidarietà per i mutui per l'acquisto della prima casa

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Consultazione; Uso; Comunicazione mediante trasmissione; Cancellazione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Dati di contatto; Dati finanziari ed economici; Dati identificativi; Dati relativi al documento d'identità; Dati relativi alla qualifica professionale, alle mansioni e alla tipologia di lavoro svolto

Qual è la finalità di trattamento?	- raccolta e protocollazione delle domande di ammissione al Fondo; - raccolta delle istanze di ammissione al Fondo; - accettazione/rigetto della richiesta di ammissione al Fondo; - pagamento oneri finanziari, interessi e rate sospese; - contestazione e/o definizione di proposte transattive; - azione di regresso nei confronti del beneficiario e recupero coattivo; - conservazione, mediante archiviazione, della documentazione; - agevolare la richiesta telefonica di informazioni da parte degli utenti e il riscontro della Società.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Contitolari mutuo; Istanti; Utenti
Quali sono i destinatari dei dati personali?	N.A.

Valutazione impatto potenziale

IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI

A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO

D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	MEDIO	2
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Fondo di solidarietà per i mutui per l'acquisto della prima casa

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**		✗	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Fondo di solidarietà per i mutui per l'acquisto della prima casa** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO

Valutazione del rischio (Responsabile)

Denominazione del Trattamento

ID: Fondo GACS004	Fondo GACS

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Consultazione; Raffronto; Uso; Cancellazione; Distruzione
Quali sono le tipologie di dati personali trattati?	Dati bancari; Dati identificativi
Qual è la finalità di trattamento?	Raccolta e lavorazione delle istanze di ammissione al fondo di garanzia e archivazione della documentazione
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Banche; Legale rappresentante
Quali sono i destinatari dei dati personali?	

Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	BASSO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	BASSO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO

B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Fondo GACS

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**	X		
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Fondo GACS** è	BASSO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO

Valutazione del rischio (Responsabile)	
Denominazione del Trattamento	
ID: FIR013	Fondo indennizzo risparmiatori (FIR)
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Uso; Comunicazione mediante trasmissione; Cancellazione; Distruzione
Quali sono le tipologie di dati personali trattati?	Altri dati: eventuali informazioni personali fornite dall'utente / richiedente; Dati bancari e/o relativi ai pagamenti; Dati di contatto; Dati di residenza / domicilio; Dati finanziari, economici e patrimoniali; Dati identificativi; Dati relativi al documento di identità (e tessera sanitaria); Dati riguardanti le persone decedute; Fascicolo personale del richiedente contenente valutazioni ed esito dell'istruttoria; Identificativi numerici o alfanumerici: credenziali di autenticazione (username e password) al Portale; Identificativi numerici o alfanumerici: numero di protocollo; Log di sistema e dati di traffico
Qual è la finalità di trattamento?	registrazione degli utenti al Portale, alla generazione e manutenzione delle credenziali di autenticazione e alla gestione degli accessi degli utenti al Portale stesso; agevolare la richiesta di informazioni da parte degli utenti e il riscontro della Società; agevolare la richiesta telefonica di informazioni da parte degli utenti e il riscontro della Società; presentazione delle richieste di indennizzo e della documentazione di supporto da parte degli istanti; protocollazione e gestione del fascicolo elettronico della domanda, di eventuali integrazioni e dei documenti allegati in conformità delle linee guida previste da AgID; esame della documentazione ricevuta e alla verifica dei requisiti per la concessione dell'indennizzo; approvazione della richiesta di indennizzo, sulla base dell'esito dell'istruttoria, e di formulazione di una proposta di liquidazione sulla quale è chiamata ad esprimersi la Commissione tecnica; comunicazione della decisione della Commissione tecnica e delle modalità di pagamento; acquisire documentazione mancante ai fini del completamento dell'istruttoria della pratica successivamente alla disabilitazione dell'operatività esterna del Portale; pagamento degli indennizzi riconosciuti; l'effettuazione di analisi e l'elaborazione di report sulle attività di lavorazione delle pratiche (dati in forma pseudonimizzata); conservazione della documentazione relativa alle pratiche lavorate.

Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Delegati; Familiari succeduti per atto inter vivos; Richiedenti; Risparmiatori richiedenti (consumatori, imprenditori individuali o agricoli, legali rappresentanti di microimprese o di organizzazione di volontariato e associazioni di promozione sociale); Successori mortis causa dei risparmiatori; Utenti; Utenti che si registrano e accedono alla Piattaforma; Visitatori della pagina web
Quali sono i destinatari dei dati personali?	N.A.
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO
Definizione delle possibili minacce e valutazione della loro probabilità	
A. RISORSE DI RETE E TECNICHE	
A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO

D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Fondo indennizzo risparmiatori (FIR)

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**		X	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Fondo indennizzo risparmiatori (FIR)** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO

Valutazione del rischio (Responsabile)	
Denominazione del Trattamento	
ID: Fondo Juncker026	Fondo Juncker (Fondo di garanzia sulle operazioni finanziarie delle piattaforme di investimento promosse dall'istituto nazionale di promozione)
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Uso; Comunicazione mediante trasmissione; Cancellazione; Distruzione
Quali sono le tipologie di dati personali trattati?	Dati finanziari ed economici; Dati identificativi
Qual è la finalità di trattamento?	- Acquisire da CDP i dati analitici delle garanzie contenute nelle piattaforme di investimento; - effettuare gli accantonamenti disposti nel decreto di approvazione della piattaforma di investimento; - gestire gli adempimenti connessi all'escussione delle garanzie; - incassare le commissioni corrisposte da CDP quale corrispettivo per il rilascio della garanzia pubblica.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Beneficiari; Richiedenti
Quali sono i destinatari dei dati personali?	
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	BASSO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	BASSO

Definizione delle possibili minacce e valutazione della loro probabilità	
A. RISORSE DI RETE E TECNICHE	
A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO

C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Fondo Juncker (Fondo di garanzia sulle operazioni finanziarie delle piattaforme di investimento promosse dall'istituto nazionale di promozione)

	Impatto			
Probabilità		**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
	BASSO	X		
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Fondo Juncker (Fondo di garanzia sulle operazioni finanziarie delle piattaforme di investimento promosse dall'istituto nazionale di promozione)** è	BASSO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO

Valutazione del rischio (Responsabile)

Denominazione del Trattamento

ID: Fondo nuovi nati021	Fondo nuovi nati

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Uso; Comunicazione mediante trasmissione; Cancellazione; Distruzione
Quali sono le tipologie di dati personali trattati?	Dati di contatto; Dati di minori; Dati finanziari, economici e patrimoniali; Dati identificativi; Dati relativi al documento d'identità; Dati sanitari
Qual è la finalità di trattamento?	- gestione dell'escussione e alla verifica della sussistenza dei requisiti dell'istante (attività già svolta dalla Banca); - contestazione (ad es. false dichiarazioni) e/o definizione di proposte transattive; - azione di regresso nei confronti del beneficiario e recupero coattivo"; - archiviazione della documentazione.

Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Banche; Istanti
Quali sono i destinatari dei dati personali?	

Valutazione impatto potenziale

IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	SI
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO

B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	MEDIO	2
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Fondo nuovi nati

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**		✗	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Fondo nuovi nati** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO

Valutazione del rischio (Responsabile)	
Denominazione del Trattamento	
ID: Fondo per gli acquirenti di beni immobili da costruire011	Fondo per gli acquirenti di beni immobili da costruire
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Estrazione; Uso; Comunicazione mediante trasmissione; Cancellazione; Distruzione
Quali sono le tipologie di dati personali trattati?	Dati bancari e/o relativi ai pagamenti; Dati di contatto; Dati identificativi; Dati relativi al documento d'identità
Qual è la finalità di trattamento?	-acquisizione e completamento delle istanze di ammissione al Fondo pregresse (Data entry); -gestione dell'archivio dati degli istanti ammessi al Fondo, le cui pratiche sono sospese fino alla re-immissione di quote nel Fondo stesso; - analisi ed istruttoria delle istanze, in caso di esito positivo è emessa una delibera di ammissione per accesso al Fondo; - pagamento degli interessati; - verifica periodica della sussistenza dei requisiti per l'utilizzo del Fondo; - alla contestazione (ad es. false dichiarazioni) e/o definizione di proposte transattive; - all'azione di regresso nei confronti del reo (costruttore) e recupero coattivo; - conservazione, mediante archiviazione, della documentazione; - agevolare la richiesta telefonica di informazioni da parte degli utenti e il riscontro della Società.
Dove ha luogo il trattamento dei dati personali?	
Quali sono le categorie di interessati coinvolti?	Imprenditori (fallito o in corso di procedura concorsuale-esecutiva); Istanti ed eredi
Quali sono i destinatari dei dati personali?	NA
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	BASSO

IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO

C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1

Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Fondo per gli acquirenti di beni immobili da costruire

	Impatto			
Probabilità		**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
	BASSO		X	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Fondo per gli acquirenti di beni immobili da costruire** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO

Valutazione del rischio (Responsabile)	
Denominazione del Trattamento	
ID: Fondo per lo studio020	Fondo per il credito ai giovani cd. "Fondo per lo studio"
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Consultazione; Uso; Cancellazione; Distruzione
Quali sono le tipologie di dati personali trattati?	Dati di contatto; Dati finanziari, economici e patrimoniali (tasse universitarie e ammontare del finanziamento richiesto); Dati identificativi; Dati relativi al documento d'identità; Dati relativi al percorso di studi
Qual è la finalità di trattamento?	- raccolta e protocollazione delle domande di ammissione al Fondo; - raccolta delle istanze di ammissione al rilascio della garanzia per accesso al credito; - accettazione/rigetto della richiesta di ammissione per erogazione del credito; - rilascio della garanzia per l'erogazione del credito previa comunicazione ricevuta dalla banca finanziatrice; - gestione dell'escussione ed alla verifica della sussistenza dei requisiti dell'istante (attività già svolta dalla Banca); - contestazione (ad es. false dichiarazioni) e/o definizione di proposte transattive; - azione di regresso nei confronti del beneficiario e recupero coattivo; - archiviazione della documentazione.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Istanti
Quali sono i destinatari dei dati personali?	
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	BASSO

IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	SI
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO

C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	MEDIO	2
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1

Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Fondo per il credito ai giovani cd. "Fondo per lo studio"

	Impatto			
Probabilità		**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
	BASSO		X	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Fondo per il credito ai giovani cd. "Fondo per lo studio"** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO

Valutazione del rischio (Responsabile)

Denominazione del Trattamento

ID: Acquisto Autobus Alta Sostenibilità Ecologica018	Incentivo per acquisto Autobus Alta Sostenibilità Ecologica

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Uso; Cancellazione; Distruzione

Quali sono le tipologie di dati personali trattati?	Dati bancari; Dati di contatto; Dati finanziari ed economici; Dati identificativi; Dati identificativi numerici e alfanumerici (password); Dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di internet tra i quali, a titolo esemplificativo, indirizzi IP o nomi a dominio dei computer utilizzati dagli utenti che si connettono alla pagina, indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente (1); Dati relativi al documento d'identità; Log di sistema e dati di traffico
Qual è la finalità di trattamento?	- accesso alla Piattaforma applicativa che consente alle autoscuole di monitorare in autonomia lo stato delle fatture inviate; - attraverso cookie tecnici (di sessione), al solo scopo di migliorare le prestazioni del sito durante la navigazione, per ottimizzare l'esperienza dell'utente nell'accesso ai servizi richiesti; - riscontro e alla liquidazione delle fatture elettroniche ricevute dagli esercenti per il rimborso dei voucher: registrazione, organizzazione, strutturazione, consultazione e raffronto, conservazione dei dati (comunicazione all'occorrenza, su richiesta); - gestione degli adempimenti previsti rispetto al RNA; - pagamento del contributo deliberato dalla Commissione ministeriale in favore del richiedente (elaborazione del mandato di pagamento massivo ed eventuale gestione di singole posizioni anomale, richiedendo alle imprese informazioni o documenti); - archiviazione della documentazione e alla conservazione delle basi di dati.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Imprese (società di persone, ditte individuali); Legale rappresentante; Titolari di ditta individuale (intestatari del c/c); Utenti che accedono al Portale
Quali sono i destinatari dei dati personali?	
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	BASSO

IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	SI
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO

C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	MEDIO	2
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1

Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Incentivo per acquisto Autobus Alta Sostenibilità Ecologica

	Impatto			
Probabilità		**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
	BASSO		X	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Incentivo per acquisto Autobus Alta Sostenibilità Ecologica** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO

Valutazione del rischio (Responsabile)	
Denominazione del Trattamento	
ID: Polizze dormienti023	Polizze dormienti
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Uso; Comunicazione mediante trasmissione; Cancellazione
Quali sono le tipologie di dati personali trattati?	Dati bancari; Dati di contatto; Dati finanziari ed economici; Dati identificativi; Dati relativi al documento d'identità
Qual è la finalità di trattamento?	- ricezione delle richieste di rimborso e documentazione a supporto; - apertura della pratica nell'archivio informatico dei rapporti dormienti e comunicazione al richiedente della presa in carico; - esame della documentazione ricevuta; - verifica della pertinenza della domanda; - verifica dell'assenza della posizione in oggetto nell'archivio informatico; - verifica della presenza dell'importo richiesto con quanto indicato sugli elenchi dei rapporti dormienti; - comunicazione al richiedente dell'accoglimento / rigetto della domanda di rimborso; - pagamento dei rimborsi; - agevolare la richiesta di informazioni sull'utilizzo del Portale Unico da parte degli utenti e il riscontro della Società; - conservazione della documentazione relativa alle pratiche lavorate.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Richiedenti (anche liquidatori, eredi)
Quali sono i destinatari dei dati personali?	
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	BASSO

IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO

C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1

Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 4

Valutazione del livello di rischio del trattamento Polizze dormienti

	Impatto			
Probabilità		**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
	BASSO		X	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Polizze dormienti** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO

Valutazione del rischio (Responsabile)

Denominazione del Trattamento

ID: Rapporti dormienti022	Rapporti dormienti

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Consultazione; Uso; Cancellazione
Quali sono le tipologie di dati personali trattati?	Dati bancari e/o relativi ai pagamenti; Dati di contatto; Dati finanziari ed economici; Dati identificativi; Dati relativi a persone defunte (eventuale) (1); Dati relativi al documento d'identità

Qual è la finalità di trattamento?	- presentazione delle richieste di rimborso e documentazione a supporto; - apertura della pratica nell'archivio informatico dei rapporti dormienti e comunicazione al richiedente della presa in carico; - esame della documentazione ricevuta; - verifica della pertinenza della domanda; - verifica dell'assenza della posizione in oggetto nell'archivio informatico; - verifica della presenza dell'importo richiesto con quanto indicato sugli elenchi dei rapporti dormienti; - verifica a campione delle pratiche istruite da CONSAP prima dell'accoglimento; - comunicazione al richiedente dell'accoglimento / rigetto della domanda di rimborso; - pagamento dei rimborsi; - agevolare la richiesta di informazioni sull'utilizzo del Portale Unico da parte degli utenti e il riscontro della Società; - archiviazione della documentazione.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Persone defunte; Richiedenti (anche legali rappresentanti di società, liquidatori, eredi)
Quali sono i destinatari dei dati personali?	
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO
Definizione delle possibili minacce e valutazione della loro probabilità	
A. RISORSE DI RETE E TECNICHE	
A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	SI

A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	MEDIO	2
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Rapporti dormienti

	Impatto		
Probabilità	**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
BASSO		X	
MEDIO			
ALTO			

Il livello di rischio del trattamento **Rapporti dormienti** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO

Valutazione del rischio (Responsabile)

Denominazione del Trattamento

ID: Ruolo dei periti assicurativi e fondo brokers005	Ruolo dei periti assicurativi e fondo brokers

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Consultazione; Uso; Comunicazione mediante trasmissione; Cancellazione; Distruzione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Altri dati: informazioni riguardanti il possesso dei requisiti richiesti dalla normativa ai fini dell'iscrizione all'Albo (sotto forma di autodichiarazione dell'interessato); Dati di contatto; Dati identificativi; Dati relativi al documento d'identità; dati relativi all'utilizzo di cookie tecnici e applicativi (con dati pseudonimizzati); Dati relativi alla qualifica professionale, alle mansioni e alla tipologia di lavoro svolto; indirizzo IP (che viene mascherato azzerando gli ultimi 2 byte); Log di sistema e dati di traffico; sistema operativo utilizzato

Qual è la finalità di trattamento?	Fondo Brokers. Trattamento di dati personali finalizzato esclusivamente al fine di svolgere le attività necessarie alla gestione della pratica risarcitoria e all'avvio delle azioni volte al recupero delle somme elargite in favore dei danneggiati, secondo quanto previsto dalla normativa che disciplina l'operatività del Fondo in questione.; Ruolo dei periti assicurativi. Trattamento di dati personali finalizzato a: - verificare l'effettivo svolgimento del periodo di tirocinio previsto dalla legge; - creazione dell'account personale e al successivo accesso all'area riservata per usufruire dei relativi servizi; - consentire la gestione delle funzionalità del Portale, a garantirne la sicurezza il corretto funzionamento e ad effettuare analisi statistiche sull'utilizzo e valutazioni di performance del sito; - iscrizione per la partecipazione all'esame di abilitazione da Periti Assicurativi RC Auto mediante presentazione della domanda attraverso le funzionalità dell'area riservata del Portale; - valutazione della prova di esame sostenuta dai candidati, anche attraverso strumenti automatizzati (prova risposta multipla); - informare i candidati dell'esito della prova di esame, mediante comunicazione resa disponibile nella loro area riservata del Portale applicativo; - ricezione ed esame della domanda di iscrizione e alla successiva pubblicazione dei dati del Perito Assicurativo nel Ruolo; - riscossione del contributo annuale, alla verifica del mantenimento dei requisiti previsti, all'irrogazione di sanzioni disciplinari, alla effettuazione di variazioni anagrafiche, ecc.; - cancellazione del Perito Assicurativo dal Ruolo; - verifica del possesso dei requisiti del perito per l'abilitazione come CTU; - recupero dei contributi annuali non versati dai Periti per l'iscrizione al Ruolo; - monitoraggio pagamento contributi d'iscrizione; - conservazione, mediante archiviazione, della documentazione (fascicolo personale del candidato e del Perito Assicurativo).
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Candidati; Interessati che presentano domanda risarcitoria; Periti Assicurativi; Utenti che si registrano e accedono al Portale; Visitatori della pagina web
Quali sono i destinatari dei dati personali?	
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MEDIO

IMPATTO SULL'INTEGRITÀ	MEDIO
IMPATTO SULLA DISPONIBILITÀ	MEDIO
Valutazione complessiva impatto (I)	MEDIO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	SI
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	MEDIO	2
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Ruolo dei periti assicurativi e fondo brokers

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**		✗	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Ruolo dei periti assicurativi e fondo brokers** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO

Valutazione del rischio (Responsabile)	
Denominazione del Trattamento	
ID: Sisma imprese025	Sisma imprese
Definizione del contesto e delle operazioni di trattamento eseguite	
Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Consultazione; Uso; Comunicazione mediante trasmissione; Cancellazione; Distruzione
Quali sono le tipologie di dati personali trattati?	Dati finanziari ed economici; Dati identificativi
Qual è la finalità di trattamento?	1. istruire le richieste di escussione trasmesse dagli istituti di credito; 2. procedere all'istruttoria delle richieste di escussione della garanzia dello Stato presentate dagli Istituti di credito direttamente al Ministero concedente ed il cui esame non sia stato ancora avviato ovvero completato; 3. disporre, all'esito dell'istruttoria, il pagamento delle escussioni sull'Iban indicato dagli istituti di credito; 4. trasmettere allo stesso Ministero tutti i dati, i documenti e le informazioni esplicative in possesso di Consap concernenti la posizione oggetto di contenzioso instaurato o minacciato, ciò anche al fine di consentire la costituzione in giudizio con il patrocinio dell'Avvocatura di Stato.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Imprese danneggiate che hanno richiesto la garanzia dello Stato
Quali sono i destinatari dei dati personali?	
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	BASSO
IMPATTO SULLA DISPONIBILITÀ	BASSO

Valutazione complessiva impatto (I)	BASSO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO

C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	NO
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	MEDIO	2
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	BASSO	1

Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Sisma imprese

	Impatto			
Probabilità		**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
	BASSO	✗		
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Sisma imprese** è	BASSO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO

Valutazione del rischio (Responsabile)

Denominazione del Trattamento

ID: Sistema di prevenzione del Furto d'Identità003	Sistema di prevenzione del Furto d'Identità

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Consultazione; Uso; Interconnessione; Comunicazione mediante trasmissione; Strutturazione
Quali sono le tipologie di dati personali trattati?	Dati finanziari ed economici; Dati identificativi; Dati previdenziali

Qual è la finalità di trattamento?	Le finalità del trattamento sono le seguenti: - acquisizione dei dati da sottoporre a verifica, alla trasmissione delle richieste di verifica all'Archivio Centrale informatizzato SCIPAFI e all'invio dei riscontri agli aderenti e ai soggetti autorizzati; - veicolazione delle richieste di interrogazione verso le banche dati di riferimento per la consultazione e alla ricezione del relativo riscontro semaforico da trasmettere agli aderenti e ai soggetti autorizzati, attraverso apposita infrastruttura informatica che gestisce l'interconnessione di reti; - stipula della convenzione con l'aderente e alla creazione, abilitazione e assegnazione, nonché variazione, delle utenze per i referenti individuati dagli aderenti; - consentire l'accesso al Portale web SCIPAFI, a monitorarne l'utilizzo da parte degli utenti abilitati degli aderenti e dei soggetti autorizzati e a controllarne il corretto funzionamento; - all'organizzazione delle riunioni (mediante convocazione dei partecipanti) e allo scambio di documenti e informazioni tra i componenti del Gruppo di lavoro; - alla gestione delle richieste di assistenza di natura amministrativa e di carattere tecnico informatico pervenute dagli aderenti e dai soggetti autorizzati; - alla gestione delle richieste di assistenza riguardanti la necessità di approfondimenti su singoli riscontri, pervenute dagli aderenti e dai soggetti autorizzati; - alla ricezione di segnalazioni da parte dei soggetti che hanno subito o temono di aver subito frodi configuranti ipotesi di furto di identità; - all'attività di archiviazione della documentazione; - al monitoraggio del servizio offerto dal Sistema SCIPAFI in generale e dalle banche dati istituzionali collegate.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Persone fisiche che hanno subito o temono di aver subito frodi identitarie; Persone fisiche la cui identità è oggetto di verifica da parte degli aderenti e dei soggetti autorizzati, con riferimento alle attività previste dalla normativa; Referenti degli aderenti
Quali sono i destinatari dei dati personali?	
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	BASSO

IMPATTO SULLA DISPONIBILITÀ	BASSO
Valutazione complessiva impatto (I)	MEDIO

Definizione delle possibili minacce e valutazione della loro probabilità

A. RISORSE DI RETE E TECNICHE

A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	NO
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	SI
A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO

B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO

C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO

C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO

D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO
D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	SI
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	MEDIO	2

Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Sistema di prevenzione del Furto d'Identità

	Impatto		
Probabilità	**BASSO**	**MEDIO**	**ALTO / MOLTO ALTO**
BASSO		X	
MEDIO			
ALTO			

Il livello di rischio del trattamento **Sistema di prevenzione del Furto d'Identità** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO / MEDIO

Valutazione del rischio (Responsabile)

Denominazione del Trattamento

ID: Stanza di Compensazione007	Stanza di Compensazione

Definizione del contesto e delle operazioni di trattamento eseguite

Quali sono le operazioni di trattamento?	Raccolta; Registrazione; Organizzazione; Conservazione; Consultazione; Estrazione; Raffronto; Uso; Interconnessione; Comunicazione mediante trasmissione; Cancellazione; Distruzione
Quali sono le tipologie di dati personali trattati?	Dati di contatto; Dati identificativi; Dati relativi ai pagamenti; Dati relativi al documento d'identità; Log di sistema e dati di traffico; Targa dell'auto

Qual è la finalità di trattamento?	- Regolazione dei rapporti credito/debito tra le Compagnie aderenti alla CARD, provvedendo al rimborso della somma pagata al danneggiato a titolo di risarcimento; - Gestione dei rapporti con i contraenti delle polizze assicurative dei veicoli responsabili per consentire il rimborso del sinistro per evitare la maggiorazione del premio per l'evoluzione del Bonus/Malus; - Consentire la gestione delle funzionalità del Portale, a garantirne la sicurezza il corretto funzionamento e ad effettuare analisi statistiche sull'utiizzo e valutazioni di performance del sito; - Agevolare la richiesta telefonica di informazioni da parte degli utenti e il riscontro della Società.
Dove ha luogo il trattamento dei dati personali?	Roma
Quali sono le categorie di interessati coinvolti?	Contraenti; Danneggiati; Imprese di assicurazione; Istanti; Utenti/Richiedenti
Quali sono i destinatari dei dati personali?	N.A.
Valutazione impatto potenziale	
IMPATTO SULLA RISERVATEZZA	MEDIO
IMPATTO SULL'INTEGRITÀ	MEDIO
IMPATTO SULLA DISPONIBILITÀ	MEDIO
Valutazione complessiva impatto (I)	MEDIO
Definizione delle possibili minacce e valutazione della loro probabilità	
A. RISORSE DI RETE E TECNICHE	
A.1 Qualche parte del trattamento dei dati personali viene eseguita tramite internet?	SI
A.2 È possibile fornire accesso a un sistema interno di trattamento dei dati personali tramite internet (ad esempio per determinati utenti o gruppi di utenti)?	NO
A.3 Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	NO

A.4 Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	NO
A.5 Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	NO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	
B.6 I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	NO
B.7 L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	NO
B.8 I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	NO
B.9 I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	NO
B.10 Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?	NO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	
C.11 Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	NO
C.12 Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	NO
C.13 Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	NO
C.14 Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	NO
C.15 Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	NO
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	
D.16 Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	NO

D.17 La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	SI
D.18 Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	NO
D.19 Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	SI
D.20 Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	NO

Probabilità minacce per area di valutazione

Area di Valutazione	Livello	Punteggio
A. RISORSE DI RETE E TECNICHE	BASSO	1
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	BASSO	1
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	BASSO	1
D. SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO	MEDIO	2
Probabilità complessiva di occorrenza minaccia (P)	BASSO	**Punteggio:** 5

Valutazione del livello di rischio del trattamento Stanza di Compensazione

		Impatto		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
Probabilità	**BASSO**		X	
	MEDIO			
	ALTO			

Il livello di rischio del trattamento **Stanza di Compensazione** è	MEDIO
è necessario applicare le misure di sicurezza Tecniche e Organizzative consigliate per il livello di rischio	BASSO MEDIO

7.1 MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

Nella complessa architettura della protezione dei dati personali, le misure tecniche e organizzative rappresentano i pilastri fondamentali per la prevenzione del rischio *privacy*. Le prime agiscono direttamente sull'infrastruttura tecnologica e sui processi di trattamento, implementando soluzioni concrete per salvaguardare la riservatezza, l'integrità e la disponibilità dei dati. Parallelamente, le misure organizzative definiscono le politiche, le procedure e le responsabilità all'interno di un'organizzazione, creando un ambiente consapevole e strutturato volto a minimizzare la probabilità di violazioni e a garantire una gestione responsabile delle informazioni personali in conformità con le normative vigenti. La sinergia tra questi due ambiti è cruciale per costruire un sistema di protezione dati robusto ed efficace.

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio per i diritti e le libertà delle persone fisiche, la Società, in qualità vuoi di Titolare vuoi di Responsabile del trattamento di dati personali, adotta misure tecniche e organizzative adeguate a garantire un livello di sicurezza commisurato al rischio.

In relazione al trattamento dei dati personali è costantemente in atto un procedimento di controllo e di verifica della sicurezza del sistema informatico attraverso l'utilizzo di appositi strumenti a livello di sistema, di gestione delle basi dati e di applicativi, effettuato anche mediante l'ausilio di soggetti terzi.

Nell'ambito del *risk assessment* svolto si è provveduto a mappare le misure di sicurezza tecniche e organizzative della Società in ambito di protezione dei dati, queste sono condivise per tutti i trattamenti. Il *driver* della mappatura è stato la divisione dei rischi delle attività di trattamento, difatti le misure di sicurezza sono maggiormente complesse all'aumentare del rischio del trattamento.

Si riporta di seguito l'elenco delle misure implementate per le aree di rischio considerate (Basso, Medio e Alto) secondo la metodologia ENISA:

Misure di sicurezza IMPLEMENTATE (42 / 46) Livello di Rischio BASSO		
CATEGORIA	**DESCRIZIONE**	**RIF. ISO 27001:2013**
Politica di sicurezza e procedure per la protezione dei dati personali	L'organizzazione dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.	A.5 Politica di sicurezza
Politica di sicurezza e procedure per la protezione dei dati personali	La politica di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale.	A.5 Politica di sicurezza
Ruoli e responsabilità	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con le politiche di sicurezza.	A.6.1.1 Ruoli e responsabilità della sicurezza delle informazioni
Ruoli e responsabilità	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo, l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.	A.6.1.1 Ruoli e responsabilità della sicurezza delle informazioni
Politica di controllo degli accessi	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.	A.9.1.1 Politica di controllo degli accessi
Gestione risorse / asset	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).	A.8 Gestione delle risorse
Gestione risorse / asset	Il censimento delle risorse e degli apparati IT e il relativo registro dovrebbero essere rivisti e aggiornati regolarmente.	A.8 Gestione delle risorse
Gestione delle modifiche	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.	A.12.1 Procedure operative e responsabilità

CATEGORIA	DESCRIZIONE	RIF. ISO 27001:2013
Gestione delle modifiche	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.	A.12.1 Procedure operative e responsabilità
Responsabili del trattamento	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.	A.15 Rapporti con i fornitori
Responsabili del trattamento	Al rilevamento di una violazione dei dati personali (*data breach*), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.	A.15 Rapporti con i fornitori
Responsabili del trattamento	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.	A.15 Rapporti con i fornitori
Gestione degli incidenti / Violazioni dei dati personali	Le violazioni dei dati personali (come definite dall'art. 4 del GDPR) devono essere segnalate immediatamente al Management competente secondo l'organizzazione interna. Dovrebbero essere in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi degli artt. 33 e 34 GDPR.	A.16 Gestione degli incidenti sulla sicurezza delle informazioni
Obblighi di confidenzialità imposti al personale	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione.	A.7 Sicurezza delle risorse umane

CATEGORIA	DESCRIZIONE	RIF. ISO 27001:2013
Formazione	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica.	A.7.2.2 Consapevolezza della sicurezza delle informazioni, educazione e formazione
Controllo degli accessi e autenticazione	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.	A.9 Controllo degli accessi
Controllo degli accessi e autenticazione	L'uso di account utente comuni (con credenziali di accesso condivise tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.	A.9 Controllo degli accessi
Controllo degli accessi e autenticazione	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.	A.9 Controllo degli accessi
Controllo degli accessi e autenticazione	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).	A.9 Controllo degli accessi
Generazione di file di log e monitoraggio	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).	A.12.4 Registrazione e monitoraggio
Generazione di file di log e monitoraggio	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento.	A.12.4 Registrazione e monitoraggio
Sicurezza server / database	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR).	A.12 Sicurezza delle operazioni

CATEGORIA	DESCRIZIONE	RIF. ISO 27001:2013
Sicurezza delle postazioni di lavoro	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.	A.14.1 Requisiti di sicurezza dei sistemi di informazione
Sicurezza delle postazioni di lavoro	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.	A.14.1 Requisiti di sicurezza dei sistemi di informazione
Sicurezza delle postazioni di lavoro	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	A.14.1 Requisiti di sicurezza dei sistemi di informazione
Sicurezza delle postazioni di lavoro	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.	A.14.1 Requisiti di sicurezza dei sistemi di informazione
Sicurezza delle postazioni di lavoro	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.	A.14.1 Requisiti di sicurezza dei sistemi di informazione
Sicurezza rete / comunicazione	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).	A.13 Sicurezza delle comunicazioni
Backup	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	A.12.3 Back-Up
Backup	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	A.12.3 Back-Up
Backup	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.	A.12.3 Back-Up
Backup	I backup completi devono essere eseguiti regolarmente.	A.12.3 Back-Up
Dispositivi mobili / portatili	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	A.6.2 Dispositivi mobili e telelavoro
Dispositivi mobili / portatili	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.	A.6.2 Dispositivi mobili e telelavoro
Dispositivi mobili / portatili	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.	A.6.2 Dispositivi mobili e telelavoro

CATEGORIA	DESCRIZIONE	RIF. ISO 27001:2013
Sicurezza del ciclo di vita delle applicazioni	Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto
Sicurezza del ciclo di vita delle applicazioni	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto
Sicurezza del ciclo di vita delle applicazioni	Dovrebbero essere seguiti standard e pratiche di codifica sicure.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto
Sicurezza del ciclo di vita delle applicazioni	Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto
Cancellazione / eliminazione dei dati	La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica.	A.8.3.2 Smaltimento di supporti e A.11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura
Cancellazione / eliminazione dei dati	È necessario eseguire la triturazione della carta e dei supporti portatili utilizzati per memorizzare i dati personali.	A.8.3.2 Smaltimento di supporti e A.11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura
Sicurezza fisica	Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile da personale non autorizzato.	A.11 Sicurezza fisica e ambientale

Misure di sicurezza IMPLEMENTATE (35 / 47)
Livello di Rischio MEDIO

CATEGORIA	DESCRIZIONE	RIF. ISO 27001:2013
Politica di sicurezza e procedure per la protezione dei dati personali	L'organizzazione dovrebbe documentare una policy di sicurezza dedicata separata per quanto riguarda il trattamento dei dati personali. La policy deve essere approvata dal management competente e comunicata a tutti i dipendenti, persone autorizzate al trattamento e alle parti esterne interessate.	A.5 Politica di sicurezza

CATEGORIA	DESCRIZIONE	RIF. ISO 27001:2013
Politica di sicurezza e procedure per la protezione dei dati personali	La policy di sicurezza dovrebbe almeno riferirsi a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, i responsabili del trattamento dei dati o altre terze parti coinvolte nel trattamento dei dati personali.	A.5 Politica di sicurezza
Politica di sicurezza e procedure per la protezione dei dati personali	Dovrebbe essere creato e mantenuto un inventario di policy / procedure specifiche relative alla sicurezza dei dati personali, basato sulla policy generale di sicurezza.	A.5 Politica di sicurezza
Ruoli e responsabilità	Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.	A.6.1.1 Ruoli e responsabilità della sicurezza delle informazioni
Politica di controllo degli accessi	Dovrebbe essere dettagliata e documentata una politica di controllo degli accessi. L'organizzazione dovrebbe determinare in questo documento le regole di controllo appropriate degli accessi, i diritti di accesso e le restrizioni per specifici ruoli degli utenti nell'ambito dei processi e delle procedure relative ai dati personali.	A.9.1.1 Politica di controllo degli accessi
Politica di controllo degli accessi	Dovrebbe essere chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).	A.9.1.1 Politica di controllo degli accessi
Gestione risorse / asset	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	A.8 Gestione delle risorse
Gestione delle modifiche	Dovrebbe essere prevista e applicata una policy interna che disciplini la gestione delle modifiche e che includa per lo meno: un processo che governi l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche dovrebbe essere regolarmente aggiornata.	A.12.1 Procedure operative e responsabilità
Responsabili del trattamento	L'organizzazione del titolare del trattamento dovrebbe svolgere regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi.	A.15 Rapporti con i fornitori

CATEGORIA	DESCRIZIONE	RIF. ISO 27001:2013
Obblighi di confidenzialità imposti al personale	Prima di assumere i propri compiti, i dipendenti, lavoratori e persone autorizzate al trattamento dovrebbero essere invitati a rivedere e concordare le policy di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.	A.7 Sicurezza delle risorse umane
Formazione	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici per l'introduzione (alle questioni di protezione dei dati) dei nuovi arrivati.	A.7.2.2 Consapevolezza della sicurezza delle informazioni, educazione e formazione
Controllo degli accessi e autenticazione	Dovrebbe essere definita e documentata una policy specifica per la password. La policy deve includere almeno la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili.	A.9 Controllo degli accessi
Controllo degli accessi e autenticazione	Le password degli utenti devono essere memorizzate in una forma "hash".	A.9 Controllo degli accessi
Generazione di file di log e monitoraggio	Le azioni degli amministratori di sistema e degli operatori di sistema, comprese le aggiunte / cancellazioni / modifiche dei diritti utente, dovrebbero essere registrate (log).	A.12.4 Registrazione e monitoraggio
Generazione di file di log e monitoraggio	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. Anche l'accesso ai file di registro dovrebbe essere registrato oltre al monitoraggio per rilevare attività insolite.	A.12.4 Registrazione e monitoraggio
Sicurezza server / database	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.	A.12 Sicurezza delle operazioni
Sicurezza server / database	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità di archiviazione.	A.12 Sicurezza delle operazioni
Sicurezza delle postazioni di lavoro	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.	A.14.1 Requisiti di sicurezza dei sistemi di informazione

CATEGORIA	DESCRIZIONE	RIF. ISO 27001:2013
Sicurezza rete / comunicazione	In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.	A.13 Sicurezza delle comunicazioni
Backup	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.	A.12.3 Back-Up
Backup	I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.	A.12.3 Back-Up
Backup	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi.	A.12.3 Back-Up
Dispositivi mobili / portatili	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.	A.6.2 Dispositivi mobili e telelavoro
Sicurezza del ciclo di vita delle applicazioni	Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture dovrebbero essere eseguiti da una terza parte certificata prima dell'adozione operativa. L'applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto
Sicurezza del ciclo di vita delle applicazioni	Devono essere eseguiti test periodici di penetrazione.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto
Sicurezza del ciclo di vita delle applicazioni	Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto
Sicurezza del ciclo di vita delle applicazioni	Le patch software dovrebbero essere testate e valutate prima di essere installate in un ambiente operativo.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto

CATEGORIA	DESCRIZIONE	RIF. ISO 27001:2013
Cancellazione / eliminazione dei dati	Se i servizi di una terza parte vengono utilizzati per smaltire in modo sicuro i documenti su supporti o supporti cartacei, dovrebbe essere stipulato un contratto di servizio e prodotto un registro della distruzione dei documenti in modo appropriato.	A.8.3.2 Smaltimento di supporti e A.11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura
Sicurezza fisica	Identificazione chiara, tramite mezzi appropriati, ad es. I badge identificativi, per tutto il personale e i visitatori che accedono ai locali dell'organizzazione, dovrebbero essere stabiliti, a seconda dei casi.	A.11 Sicurezza fisica e ambientale
Sicurezza fisica	Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Un registro fisico o una traccia elettronica di controllo di tutti gli accessi dovrebbero essere mantenuti e monitorati in modo sicuro.	A.11 Sicurezza fisica e ambientale
Sicurezza fisica	I sistemi di rilevamento anti-intrusione dovrebbero essere installati in tutte le zone di sicurezza.	A.11 Sicurezza fisica e ambientale
Sicurezza fisica	Se del caso, dovrebbero essere costruite barriere fisiche per impedire l'accesso fisico non autorizzato.	A.11 Sicurezza fisica e ambientale
Sicurezza fisica	Le aree sicure non occupate devono essere fisicamente chiuse a chiave e periodicamente riesaminate.	A.11 Sicurezza fisica e ambientale
Sicurezza fisica	Un sistema antincendio automatico, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di continuità (UPS) dovrebbero essere attivati nella sala server.	A.11 Sicurezza fisica e ambientale
Sicurezza fisica	Il personale di servizio di supporto esterno deve avere accesso limitato alle aree protette.	A.11 Sicurezza fisica e ambientale

Misure di sicurezza IMPLEMENTATE (13 / 25) Livello di Rischio ALTO		
CATEGORIA	**DESCRIZIONE**	**RIF. ISO 27001:2013**
Ruoli e responsabilità	Il responsabile della sicurezza dovrebbe essere nominato formalmente (documentato). Anche i compiti e le responsabilità del responsabile della sicurezza dovrebbero essere chiaramente definiti e documentati.	A.6.1.1 Ruoli e responsabilità della sicurezza delle informazioni
Ruoli e responsabilità	Compiti e responsabilità in conflitto, ad esempio i ruoli di responsabile della sicurezza, revisore della sicurezza e DPO, dovrebbero essere considerati separatamente per ridurre le ipotesi di modifiche non autorizzate o non intenzionali o un uso improprio di dati personali.	A.6.1.1 Ruoli e responsabilità della sicurezza delle informazioni
Politica di controllo degli accessi	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff.	A.9.1.1 Politica di controllo degli accessi
Responsabili del trattamento	I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi documentati di riservatezza / non divulgazione.	A.15 Rapporti con i fornitori
Gestione degli incidenti / Violazioni dei dati personali	Gli incidenti e le violazioni dei dati personali devono essere registrati insieme ai dettagli riguardanti l'evento e le successive azioni di mitigazione intraprese.	A.16 Gestione degli incidenti sulla sicurezza delle informazioni
Business continuity	Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.	A.17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa
Obblighi di confidenzialità imposti al personale	I dipendenti coinvolti nel trattamento dei dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale).	A.7 Sicurezza delle risorse umane
Formazione	Dovrebbe essere predisposto ed eseguito su base annuale un piano di formazione con scopi e obiettivi definiti.	A.7.2.2 Consapevolezza della sicurezza delle informazioni, educazione e formazione
Controllo degli accessi e autenticazione	L'autenticazione dei dispositivi dovrebbe essere utilizzata per garantire che il trattamento dei dati personali sia effettuato solo attraverso risorse specifiche nella rete.	A.9 Controllo degli accessi

CATEGORIA	DESCRIZIONE	RIF. ISO 27001:2013
Sicurezza delle postazioni di lavoro	Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).	A.14.1 Requisiti di sicurezza dei sistemi di informazione
Sicurezza delle postazioni di lavoro	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.	A.14.1 Requisiti di sicurezza dei sistemi di informazione
Dispositivi mobili / portatili	Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte).	A.6.2 Dispositivi mobili e telelavoro
Dispositivi mobili / portatili	I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati.	A.6.2 Dispositivi mobili e telelavoro

In un'ottica di pianificazione e prioritizzazione sono state mappate anche le misure di sicurezza in fase di implementazione o non ancora implementate.
Inoltre, tale mappatura è rilevante ai fini del rispetto:

- dell'Art. 5 del GDPR *sull'Accountability* che richiede al Titolare del trattamento di dimostrare la conformità al GDPR;
- dell'Art. 32 del GDPR sulla valutazione de rischi, al fine di valutare il rischio residuo;
- degli Artt. 33 e 34 del GDPR sulla gestione degli incidenti di sicurezza, poiché in caso di violazione dei dati tali misure possono essere utili per l'analisi della causa della violazione;
- dell'Art. 39 del GDPR, difatti tale mappatura agevola i compiti di monitoraggio del DPO.

Si riportano di seguito le misure di sicurezza in fase di implementazione divise per rischio:

Misure di sicurezza IN FASE DI IMPLEMENTAZIONE Livello di Rischio BASSO		
CATEGORIA	**DESCRIZIONE**	**RIF. ISO 27001:2013**
Gestione degli incidenti / Violazioni dei dati personali	È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.	A.16 Gestione degli incidenti sulla sicurezza delle informazioni
Business continuity	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).	A.17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa
Sicurezza server / database	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.	A.12 Sicurezza delle operazioni
Sicurezza del ciclo di vita delle applicazioni	Le tecnologie e le tecniche specifiche progettate per supportare la *privacy* e la protezione dei dati (denominate anche tecnologie di miglioramento della *privacy* (PET)) dovrebbero essere adottate in analogia con i requisiti di sicurezza.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto

Misure di sicurezza IN FASE DI IMPLEMENTAZIONE Livello di Rischio MEDIO		
CATEGORIA	**DESCRIZIONE**	**RIF. ISO 27001:2013**
Gestione degli incidenti / Violazioni dei dati personali	Il piano di risposta degli incidenti (Incident Response Plan) dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	A.16 Gestione degli incidenti sulla sicurezza delle informazioni
Business continuity	Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	A.17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa

CATEGORIA	DESCRIZIONE	RIF. ISO 27001:2013
Business continuity	Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi aziendali fondamentali che attengono alla sicurezza dei dati personali.	A.17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa
Generazione di file di log e monitoraggio	Un sistema di monitoraggio dovrebbe elaborare i file di log e produrre report sullo stato del sistema e notificare potenziali allarmi.	A.12.4 Registrazione e monitoraggio
Sicurezza server / database	Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato senza ulteriori informazioni.	A.12 Sicurezza delle operazioni
Sicurezza rete / comunicazione	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.	A.13 Sicurezza delle comunicazioni
Sicurezza rete / comunicazione	Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.	A.13 Sicurezza delle comunicazioni
Backup	Se viene utilizzato un servizio di terze parti per l'archiviazione di backup, la copia deve essere crittografata prima di essere trasmessa dal titolare del trattamento.	A.12.3 Back-Up
Dispositivi mobili / portatili	L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile che è stato compromesso.	A.6.2 Dispositivi mobili e telelavoro
Dispositivi mobili / portatili	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.	A.6.2 Dispositivi mobili e telelavoro
Dispositivi mobili / portatili	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.	A.6.2 Dispositivi mobili e telelavoro
Cancellazione / eliminazione dei dati	Più passaggi di sovrascrittura basata su software devono essere eseguiti su tutti i supporti prima di essere smaltiti.	A.8.3.2 Smaltimento di supporti e A.11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura

Misure di sicurezza IN FASE DI IMPLEMENTAZIONE Livello di Rischio ALTO		
CATEGORIA	**DESCRIZIONE**	**RIF. ISO 27001:2013**
Politica di sicurezza e procedure per la protezione dei dati personali	Le policy di sicurezza dovrebbero essere riviste e corrette, se necessario, su base semestrale.	A.5 Politica di sicurezza
Gestione risorse / asset	Le risorse IT dovrebbero essere riviste e aggiornate su base annuale.	A.8 Gestione delle risorse
Business continuity	Dovrebbe essere nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati personali.	A.17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa
Controllo degli accessi e autenticazione	L'autenticazione a due fattori (autenticazione forte) dovrebbe preferibilmente essere implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.	A.9 Controllo degli accessi
Sicurezza server / database	Dovrebbero essere considerate le tecniche che supportano la *privacy* a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della *privacy*, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc.	A.12 Sicurezza delle operazioni
Sicurezza delle postazioni di lavoro	Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali.	A.14.1 Requisiti di sicurezza dei sistemi di informazione
Sicurezza rete / comunicazione	La connessione a Internet non dovrebbe essere consentita ai server e alle postazioni di lavoro utilizzate per il trattamento dei dati personali.	A.13 Sicurezza delle comunicazioni
Sicurezza rete / comunicazione	La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati.	A.13 Sicurezza delle comunicazioni
Sicurezza rete / comunicazione	L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC).	A.13 Sicurezza delle comunicazioni

CATEGORIA	DESCRIZIONE	RIF. ISO 27001:2013
Backup	Le copie dei backup dovrebbero essere crittografate e archiviate in modo sicuro, anche offline.	A.12.3 Back-Up
Cancellazione / eliminazione dei dati	Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.	A.8.3.2 Smaltimento di supporti e A.11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura
Cancellazione / eliminazione dei dati	Se è una terza parte, (quindi un responsabile del trattamento) ad occuparsi della distruzione di supporti o file cartacei, il processo si dovrebbe svolgere presso le sedi del titolare del trattamento (ed evitare il trasferimento all'esterno dei dati personali).	A.8.3.2 Smaltimento di supporti e A.11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura

8. VALUTAZIONE D'IMPATTO - DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Prima di iniziare una nuova attività di trattamento, il Responsabile della Direzione competente comunica tale circostanza al Servizio *Audit, Compliance, Risk Management e Privacy*, al fine di consentire le necessarie valutazioni – di carattere preliminare – in materia di trattamento dei dati personali, in particolare per quanto concerne gli eventuali rischi e, se del caso, la necessità di effettuare una valutazione d'impatto sulla protezione dei dati (nel seguito anche "DPIA"). Quando un tipo di trattamento, in particolare se prevede l'uso di nuove tecnologie (Art.35 del GDPR), presenta un rischio elevato per i diritti e le libertà degli Interessati, il Titolare esegue, prima di procedere al trattamento, una valutazione dell'impatto del trattamento sui Dati Personali in riferimento ai diritti e alla libertà degli Interessati, con particolare riguardo al loro diritto alla protezione dei Dati Personali.

Tale valutazione deve essere eseguita in tutti i casi nei quali una prima analisi porti a ritenere che il trattamento presenti dei rischi specifici in base alla tipologia dei dati trattati, alle caratteristiche ed alle modalità del trattamento, agli strumenti utilizzati ed alle possibili ricadute sui diritti e le libertà degli Interessati. Inoltre, una volta che la valutazione sia stata condotta sarà comunque necessario che venga aggiornata periodicamente al fine di rivedere i risultati anche in considerazione dei cambiamenti intervenuti, medio tempore, nella tipologia dei dati trattati, nelle modalità di trattamento, nelle soluzioni tecnologiche impiegate che possono aver modificato significativamente le analisi iniziali. La valutazione prende in considerazione l'intero ciclo di vita dei Dati Personali, dalla raccolta alla cancellazione e tiene conto di eventuali elementi specifici richiesti dal particolare contesto nel quale avvengono i trattamenti nonché della normativa applicabile.

9. REGOLAMENTI E PROCEDURE PRIVACY

Nel presente Modello Organizzativo *Privacy* sono stati allegati una serie di regolamenti al fine di soddisfare i principi della protezione dei dati fissati dall'art.5 del GDPR e gestire la responsabilità generale conformemente alla struttura, obiettivi e finalità della Società.

9.1 REGOLAMENTO AMMINISTRATORI DI SISTEMA

L'Amministratore di Sistema è il soggetto responsabile della gestione e manutenzione di un sistema di elaborazione e/o delle sue componenti.

Il provvedimento del Garante italiano per la Protezione dei Dati Personali del 27 novembre 2008 prevede l'adozione di adeguate misure tecniche e organizzate per la gestione del processo di nomina e verifica dell'operato degli Amministratori di Sistema.
Attività tecniche quali le attività di salvataggio dati (*backup/recovery*), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e/o la manutenzione dell'*hardware* comportano, in molti casi, la capacità di avere un impatto sulle informazioni; tale capacità dovrebbe essere equiparata, a tutti gli effetti, a un trattamento di dati personali, anche quando l'amministratore non acceda in chiaro alle informazioni. Per questo motivo si è ritenuto necessario emettere un regolamento che fissasse le principali norme interne in materia di Amministratore di Sistema al fine di garantire una corretta e sicura gestione del processo (**Allegato 2**).
L'attribuzione del ruolo di Amministratore di Sistema avviene attraverso formale designazione a cura dell'Amministratore Delegato, su proposta del Responsabile della Direzione ICT, sentito il DPO, previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto che si intende designare, il quale, a sua volta, deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati.
L'Amministratore Delegato può revocare in qualunque momento la nomina di Amministratore di Sistema.

9.2 INCIDENT MANAGEMENT

La violazione dei dati personali si configura nei casi in cui si verifica un incidente di sicurezza che comporti, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Al fine di gestire possibili incidenti relativi ai sistemi informativi aziendali (cd. *incident*), ivi comprese le violazioni sui dati personali, sono state definite le principali regole che il personale della Società è tenuto ad osservare nel processo di gestione di un incident che potrebbe materializzarsi a seguito di un evento negativo (malevolo o accidentale) in grado di inficiare la confidenzialità, l'integrità e/o la disponibilità dei sistemi informatici o delle informazioni aziendali.

**Grafico - procedura incident management*

Le regole stabilite si applicano ogniqualvolta si verifichi un *incident* che coinvolga i sistemi informatici dell'azienda e si rivolgono indistintamente a dipendenti, consulenti e terze parti in generale, nei limiti in cui siano affidatari di responsabilità o svoltano attività pertinenti all'ambito sopra indicato.

La notifica dell'incident che interessi i sistemi informativi aziendali può essere effettuata da un qualunque utente/dipendente che, a seconda della casistica rilevata, notifica l'anomalia tramite lo strumento di ticketing o rivolgendosi al primo livello di help desk, laddove esistente. La rilevazione dell'incident perviene in ogni caso all'addetto Servizio Sistemi Informativi. Nel solo caso di incident infrastrutturali, la rilevazione viene di norma effettuata automaticamente da specifici strumenti di monitoraggio o manualmente da verifiche periodiche svolte dall'addetto dedicato. Quest'ultimo effettua sempre una valutazione ed assegna priorità all'evento ma, solo nel caso in cui l'incident riguardi dati personali, informa il Titolare del Servizio Sistemi informativi che coinvolge il DPO al fine di valutare se si sia verificato o meno un *data breach* , in conformità all'apposito Regolamento aziendale "Individuazione e notificazione *Data Breach*" che verrà trattata nel prossimo paragrafo.

9.3 REGOLAMENTO DATA BREACH

In caso di una violazione di dati personali la Società adotta misure organizzative adeguate, stabilendo ruoli e responsabilità chiari e garantendo flussi informativi appropriati tra le diverse funzioni coinvolte. Queste misure assicurano che ogni violazione di dati personali

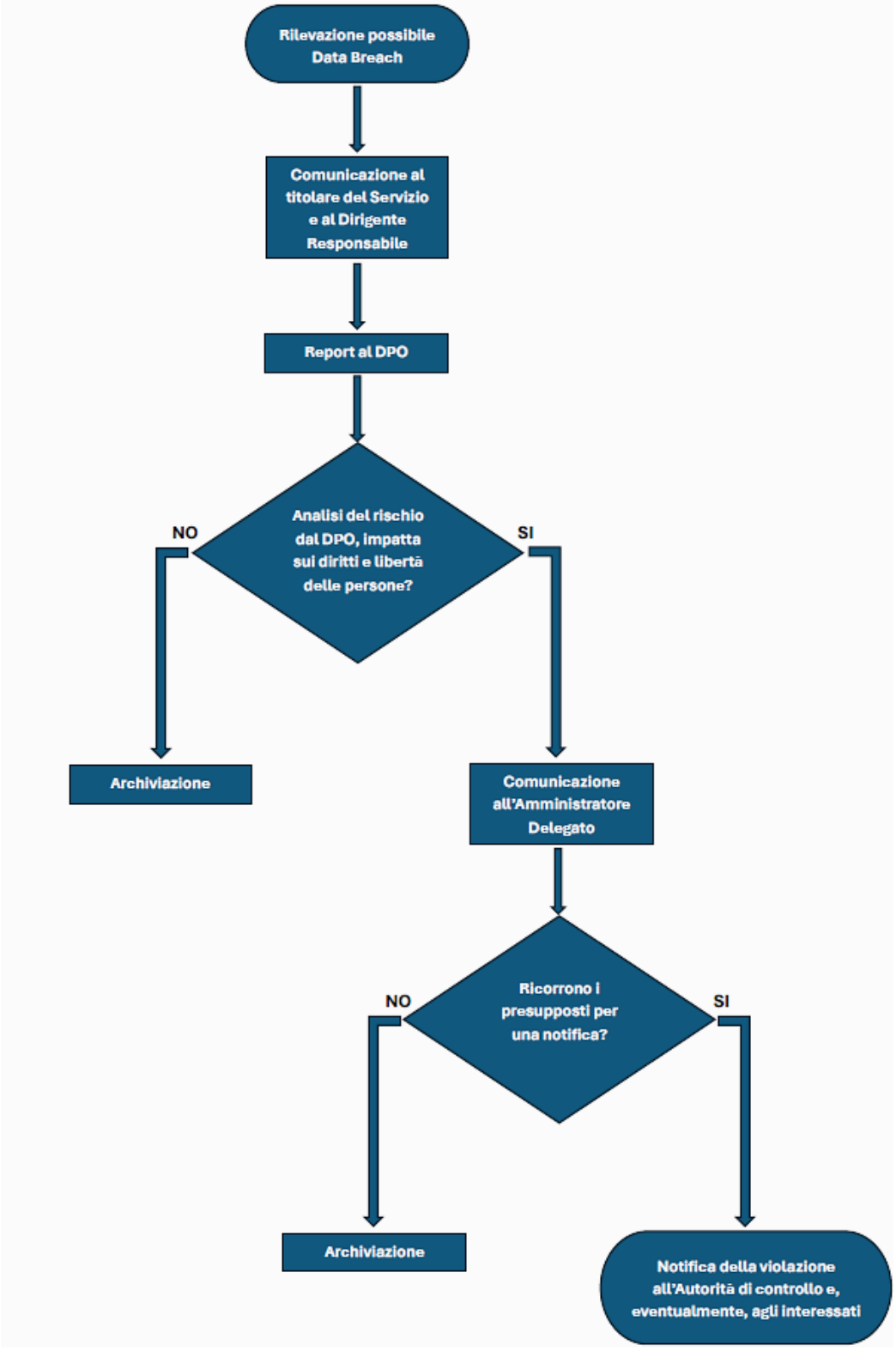
venga tempestivamente individuata, valutata, notificata e tracciata, in conformità con le disposizioni del Regolamento.

Gli adempimenti in oggetto riguardano:

- individuazione della tipologia di violazione intervenuta;
- effettuazione di una valutazione del rischio conseguente al *Data Breach* al fine di individuare le misure volte ad arginare od eliminare l'intrusione e di valutare la necessità di attivare le procedure di comunicazione e di notifica;
- notificazione della violazione dei dati personali all'Autorità di Controllo e comunicazione agli interessati, qualora il rischio per i diritti e le libertà delle persone fisiche sia considerato elevato;
- documentazione delle violazioni di dati personali occorse tenendo aggiornato un apposito registro.

La Società ha adottato un apposito Regolamento che disciplina le procedure interne da seguire in caso di *Data Breach (***Allegato 3***)*.

**Schema d'azione in caso di data breach*



Nella tabella seguente viene proposta la matrice delle responsabilità dei ruoli/funzioni coinvolte nella procedura *Data Breach*.

** matrice delle responsabilità Data Breach*

LEGENDA: **R** --> responsabile dell'attività **A** --> approva l'attività **S** --> supporta la realizzazione	*Dipendente (di ogni ordine e grado)*	*DPO*	*SACRMP*	*Titolare di Servizio/Dirigente Responsabile*	*Amministratore Delegato*
Procedura di gestione e valutazione del data breach					
Segnalazione della violazione	R			R	
Attività istruttoria: raccolta di informazioni e prima individuazione misure correttive / riparatorie / di ripristino				R	
Analisi del rischio e valutazione sulla necessità, o meno, di procedere alla notifica all'autorità di controllo e alla comunicazione all'interessato		R	S		
Approvazione in merito alla notifica all'autorità di controllo e alla comunicazione all'interessato					A
Notifica di una violazione all'autorità di controllo					
Predisposizione della comunicazione indirizzata all'autorità di controllo ai fini della notifica		R	S	S	
Validazione del contenuto della notifica indirizzata all'autorità di controllo		R	S		A
Trasmissione della notifica all'autorità di controllo		R	S		A
Comunicazione di una violazione all'interessato					
Predisposizione della comunicazione indirizzata all'interessato		R	S		
Validazione del contenuto della comunicazione indirizzata all'interessato		R	S		A
Trasmissione della comunicazione all'interessato				R	R
Obbligo di documentazione					
Documentazione dell'iter valutativo – decisionale e successivo riporto al Consiglio di Amministrazione		S	R		
Archiviazione comunicazioni inviate all'autorità di controllo e all'interessato			R		
Alimentazione del registro		R			
Conservazione del registro		R	R		

9.4 REGOLAMENTO DIRITTI INTERESSATI

In base a quanto previsto dal Regolamento (**Allegato 4**), la Società, in qualità di Titolare del trattamento dei dati personali, deve mettere a disposizione dell'interessato tutte le informazioni e comunicazioni riguardanti il trattamento in modo chiaro, comprensibile e facilmente accessibile, utilizzando un linguaggio semplice. Queste informazioni vanno fornite per iscritto o, se opportuno, anche attraverso strumenti elettronici. Su richiesta dell'interessato, possono essere comunicate anche verbalmente, a condizione che l'identità dell'interessato sia confermata con altri mezzi. La Società agevola l'esercizio di tali diritti da parte dell'interessato, con particolare riferimento a:

- *diritto di accesso*: ovvero il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati che lo riguardano e, in tal caso, di ottenere l'accesso a tali dati personali, ottenendone copia ai sensi dell'art. 15 del Regolamento;

- *diritto di rettifica*: ovvero il diritto di ottenere la rettifica dei dati inesatti che lo riguardano o l'integrazione dei dati incompleti;

- *diritto alla cancellazione* («diritto all'oblio»): ovvero il diritto di ottenere la cancellazione dei dati che lo riguardano, se sussiste uno dei motivi indicati dall'art. 17 del Regolamento;

- *diritto di limitazione di trattamento*: ovvero il diritto di ottenere, nei casi indicati dall'art.18 del Regolamento, la cancellazione/pseudonimizzazione/anonimizzazione dei dati personali che lo riguardano con l'obiettivo di limitarne il trattamento;

- *diritto alla portabilità dei dati*: ovvero il diritto, nei casi indicati dall'art. 20 del Regolamento, di ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati che lo riguardano, nonché di trasmettere tali dati ad un altro titolare del trattamento senza impedimenti;

- *diritto di opposizione*: ovvero il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, compresa la profilazione sulla base di tali disposizioni;

- *processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*: ovvero il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, salvo i casi previsti dall'art. 22 del Regolamento.

Al fine di garantire il rispetto dei diritti degli interessati Consap si è dotata di un proprio Regolamento al fine di consentire agli interessati di poter formulare le proprie richieste.

10. INFORMAZIONE E FORMAZIONE

L'obiettivo di garantire un corretto trattamento dei dati, conforme ai requisiti previsti dalla normativa, viene raggiunto dalla Consap S.p.A. anche e soprattutto grazie alla particolare

attenzione riposta nei confronti della formazione del proprio personale. Il MOP viene divulgato presso il personale in servizio ed eventuali aggiornamenti sono diffusi con gli strumenti ritenuti di volta in volta più efficaci. Tale approccio mira a creare un ambiente di lavoro in cui la consapevolezza e la responsabilizzazione in materia di protezione dei dati personali siano parte integrante della cultura aziendale. La formazione continua rappresenta infatti un elemento chiave per prevenire comportamenti non conformi e per assicurare che ogni attività venga svolta nel rispetto dei principi di liceità, correttezza e trasparenza. Attraverso sessioni formative periodiche, materiali informativi mirati e momenti di confronto con le funzioni preposte, la Società intende rafforzare le competenze dei propri dipendenti, affinché ciascuno sia in grado di riconoscere i rischi legati al trattamento dei dati e di adottare le misure adeguate a mitigarli. Questa strategia formativa si affianca a un sistema di monitoraggio e controllo interno, volto a verificare l'effettiva applicazione delle disposizioni contenute nel MOP e nelle normative vigenti, promuovendo così un miglioramento continuo in ambito *privacy* e sicurezza delle informazioni.

Inoltre, i dipendenti della Consap S.p.A. potranno fare riferimento al Servizio *audit, compliance, risk management* e *privacy* o direttamente al DPO per la proposta di quesiti o la richiesta di approfondimenti.

11. GESTIONE E AGGIORNAMENTO DEL MOP

L'aggiornamento del MOP è curato dal Servizio *Audit, Compliance, Risk Management e Privacy*, che, successivamente, richiede apposito parere al competente DPO.

La revisione periodica viene effettuata secondo il cd. *Ciclo di Deming*, cioè un processo iterativo di miglioramento continuo basato su un ciclo di quattro fasi: pianificazione (PLAN), attuazione (DO), verifica e riesame (CHECK) e aggiornamento e attuazione (ACT).

**Ciclo di Deming*

Pertanto, il presente MOP prevede che il titolare del trattamento in applicazione:

a. dell'art. 25 del GDPR (che pone il principio di *privacy* by design), pianifichi (PLAN) l'adozione di misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati fissati dall'art. 5 GDPR;
b. dell'art. 24 par. 1 del GDPR, metta in atto (DO) le misure pianificate per garantire, ed essere in grado di dimostrare, che i processi aziendali in cui girano dati personali sono effettivamente allineati ai citati principi fonda mentali;
c. dell'art. 24, par. 1 del GDPR, verifichi e riesamini (CHECK) le misure adottate;
d. dell'art. 24, porti a maturazione il ciclo, aggiornando le misure adottate e definendo ed implementando politiche e procedure (ACT).

ALLEGATI

1. Policy Data Protection;
2. Regolamento amministratori di sistema;
3. Regolamento individuazione e notificazione Data Breach;
4. Regolamento Esercizio dei diritti degli Interessati ai sensi del Regolamento UE 2016/679.