ENTE DI GOVERNO DELL'AMBITO DELLA SARDEGNA

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE[1] (PPD) aggiornamento 2025-2027

approvato in adeguamento della norma UNI ISO 31000
e conforme al REGOLAMENTO UE 2016/679

[1] Il paragrafo 5.5.3 della norma UNI ISO 31000 prevede la predisposizione e l'adeguamento di "PIANI DI TRATTAMENTO DEL RISCHIO" aventi lo scopo di documentare come le opzioni di trattamento scelte sono attuate e indica, altresì, le informazioni da fornire nei suddetti piani.

Sommario

PREMESSA 5

PARTE I 6

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE (PPD) 6

DEFINIZIONI 6

QUADRO NORMATIVO DI RIFERIMENTO 8

DATA E PROVVEDIMENTO DI APPROVAZIONE 9

PERIODO DI RIFERIMENTO E MODALITÀ DI AGGIORNAMENTO 9

ATTORI INTERNI ALL'AMMINISTRAZIONE CHE HANNO PARTECIPATO ALLA PREDISPOSIZIONE DEL PIANO, NONCHÈ CANALI E STRUMENTI DI PARTECIPAZIONE 9

CANALI, STRUMENTI E INIZIATIVE DI COMUNICAZIONE DEI CONTENUTI 10

PARTE II 10

DATI PERSONALI, RISCHIO DI VIOLAZIONE E DISCIPLINA DEL GDPR 10

IL RISCHIO PER I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI E LA NEUTRALIZZAZIONE DEL RISCHIO ATTRAVERSO IL SISTEMA DI PROTEZIONE 10

L'ACCOUNTABILITY QUALE CONSEGUENZA DELL'APPROCCIO BASATO SUL RISCHIO 11

L'INFORMATIVA 12

Contenuti dell'informativa 12

Tempi dell'informativa 13

Modalità dell'informativa 13

I DIRITTI DEGLI INTERESSATI 14

Diritto di accesso 14

Diritto alla rettifica e cancellazione 15

Diritto alla limitazione 16

Diritto alla portabilità 16

Diritto di opposizione e processo decisionale automatizzato relativo alle persone 17

PARTE III 18

CONTESTO, SOGGETTI RESPONSABILI, SICUREZZA E DOCUMENTAZIONE DEL SISTEMA DI PROTEZIONE 18

IL CONTESTO DEL SISTEMA DI PROTEZIONE 18

I SOGGETTI E LE RESPONSABILITÀ 18

Titolare del trattamento 18

Contitolari del trattamento 18
Responsabili del trattamento e sub-responsabili 19
Autorizzati al trattamento (incaricati) 20
Raccomandazioni del Garante su titolare, responsabile e incaricato del trattamento 20
Responsabile della protezione dei dati (RPD/DPO) 21
LA SICUREZZA 22
Misure di sicurezza 22
Codici di condotta 22
Certificazione 23
Notifica di una violazione dei dati personali all'Autorità di controllo 23
Comunicazione di una violazione dei dati personali all'interessato 24
PARTE IV 25
GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000 25
Principi applicabili alla gestione del rischio 25
GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000: FASE DELLA ANALISI 25
Contesto interno gestionale e operativo 28
Contesto esterno: trattamenti effettuati da responsabili esterni e titolati autonomi 29
PARTE V 29
GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000: FASE DELLA VALUTAZIONE 29
Determinazione di assoggettabilità dei trattamenti a valutazione di impatto - DPIA 29
PARTE VI 31
GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000: FASE DEL TRATTAMENTO 31
Misure di sicurezza del trattamento 31
Misure di sicurezza logistiche 32
Misure di sicurezza informatiche 34
Misure di sicurezza organizzative 35
Misure di sicurezza procedurali 36
Piano formativo 37
Social network 38
Posta elettronica e internet 38

Whistleblowing 39

ALLEGATI 41

Numero di versione: 06

Data ultimo aggiornamento: 16.07.2025

Stato del documento: Approvato da titolare con proprio provvedimento

Estensore del documento: Ente di Governo dell'Ambito della Sardegna

Riferimento per comunicazioni in merito al documento: Via Cesare Battisti 14 - 09123 Cagliari - PEC: protocollo@pec.egas.sardegna.it

Modalità di distribuzione del presente documento e delle eventuali nuove versioni: Pubblicazione sul sito istituzionale e nella sezione “Amministrazione trasparente”

PREMESSA

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell''Unione europea ("Carta") e l'articolo 16, paragrafo 1, del Trattato sul funzionamento dell''Unione europea ("TFUE") stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

Le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche.

Occorre tuttavia considerare che la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

Tale evoluzione ha indotto l'Unione europea ad adottare il GDPR (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 (GDPR generale sulla protezione dei dati, di seguito solo GDPR).

Con il GDPR è stato richiesto agli Stati membri un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, data l'importanza di creare il clima di fiducia funzionale allo sviluppo dell'economia digitale in tutto il mercato interno.

In adeguamento al GDPR, il presente Piano di protezione dei dati personali (PPD) intende rappresentare il fulcro del sistema di protezione.

PARTE I
PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE (PPD)

DEFINIZIONI

Il presente documento recepisce e utilizza le seguenti definizioni:

- "GDPR": il 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 (GDPR generale sulla protezione dei dati);
- "WP29": gruppo di lavoro articolo 29 sulla protezione dei dati, per tale dovendosi intendere il Gruppo di lavoro istituito in virtù dell'articolo 29 della direttiva 95/46/CE quale organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata con i suoi compiti fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE;
- "PPD": il presente Piano di Protezione dei Dati personali e gestione del rischio di violazione;
- "Regolamento sulla protezione dei dati personali": il Regolamento interno, approvato dal titolare, che identifica e rende pubblici, per i trattamenti dei dati personali, compresi quelli sensibili e giudiziari, i tipi di dati e le operazioni eseguibili;
- "ID": identificativo.

Recepisce e utilizza, altresì, le seguenti definizioni:

- "dato personale": 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 del 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 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 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;
- “destinatario”: la persona fisica o giuridica, l'autorità pubblica, il servizio o 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 ed 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;

OGGETTO E FINALITÀ

Il PPD individua le politiche, gli obiettivi strategici e gli standard di sicurezza per garantire la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati personali, definendo il quadro delle misure di sicurezza informatiche/logiche, logistiche/fisiche, organizzative e procedurali da adottare e da applicare per ridurre/eliminare il RISCHIO di violazione dei dati derivante dal trattamento.

In tale quadro, il documento disciplina, secondo i principi della UNI ISO 31000:2018, il sistema di gestione del trattamento dei dati personali e il rischio di violazione dei dati personali medesimi. La disciplina si applica ai:

- trattamenti con strumenti elettronici;
- trattamenti senza l'ausilio di strumenti elettronici (ad esempio: cartacei, audio, visivi e audiovisivi, ecc.).

Il presente documento, in attuazione del GDPR e della normativa interna di adeguamento, è funzionale alla protezione dei diritti e delle libertà fondamentali delle persone fisiche, in particolare alla protezione dei dati personali trattati nell'esercizio dell'attività istituzionale in un quadro di garanzie per gli interessati che

contempla nuovi diritti. Sul presupposto che la sicurezza del trattamento dei dati personali costituisce un obiettivo strategico, scopo del presente documento è programmare e pianificare gli interventi affinché i dati personali siano trattati conformemente ai principi dell'art. 5 del GDPR, e nello specifico:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (“liceità, correttezza e trasparenza”);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali (“limitazione della finalità”);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (“minimizzazione dei dati”);

d) utilizzati al minimo, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo un caso di necessità (“necessità”)

e) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (“esattezza”);

f) 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'adeguamento di misure tecniche e organizzative adeguate richieste dal presente GDPR a tutela dei diritti e delle libertà dell'interessato (“limitazione della conservazione”);

g) 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 (“integrità e riservatezza”).

QUADRO NORMATIVO DI RIFERIMENTO

Il PPD tiene conto dei seguenti documenti:

- D.Lgs. 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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”;
- GDPR UE 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, “Regolamento Del Parlamento Europeo 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);
- D.Lgs. 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)”, di adeguamento della normativa interna al GDPR;
- D.L. 8 ottobre 2021, n. 139 “Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali”, convertito in legge, con modificazioni, dall'art. 1, comma 1, della L. 3 dicembre 2021, n. 205, che, tra l’altro, apporta ulteriori modifiche al D.Lgs. 196/2003 di cui sopra;

- D.Lgs. 10 marzo 2023, n. 24, “Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali”, che sostituisce, a partire dal 15 luglio 2023, la lettera f) del comma 1 dell’art. 2-undecies del D.lgs. 196/2003, come dettagliato meglio nel seguito;
- D.L. 2 marzo 2024, n. 19, convertito in legge, con modificazioni, dall’art. 1, comma 1, L. 29 aprile 2024, n. 56, recante “*Ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR)*”, limitatamente all’art. 44, con cui sono state apportate modifiche all’art. 2-sexies ed all’art. 110, comma 1 del D.lgs. 196/2003, con riferimento all’ambito sanitario;
- Linee guida, raccomandazioni e altri provvedimenti del Garante;
- Dichiarazioni e Linee Guida del gruppo di lavoro articolo 29;
- Atti di regolamentazione interni.

DATA E PROVVEDIMENTO DI APPROVAZIONE

L'organo competente del titolare ha approvato il PPD 2020/2022 con Deliberazione n. 15 del 15 aprile 2020 e aggiornato lo stesso, con riferimento al periodo 2021/2023, con Deliberazione n. 40 del 28 luglio 2021, con riferimento al periodo 2022/2024 con Deliberazione n. 18 del 16 gennaio 2022, con riferimento al periodo 2023/2025 con Deliberazione n. 29 del 26 luglio 2023, e con riferimento al periodo 2024/2026 con Deliberazione n. 34 del 27 giugno 2024. L’aggiornamento del Piano con riferimento al periodo 2025/2027 è approvato con Deliberazione n. 19 del 4 agosto 2025.

PERIODO DI RIFERIMENTO E MODALITÀ DI AGGIORNAMENTO

Come sopra riportato, l’aggiornamento del Piano copre il periodo del triennio 2025-2027; la funzione principale dello stesso è quella di assicurare il processo, a ciclo continuo, di adozione, modificazione, aggiornamento e adeguamento del processo di gestione del rischio e della strategia di sicurezza, secondo i principi, le disposizioni e le linee guida elaborate a livello nazionale e internazionale.

Il documento consente che la strategia si sviluppi e si modifichi in modo da mettere progressivamente a punto degli strumenti di protezione mirati e sempre più incisivi. In questa logica, l'adozione del documento non si configura come un'attività una tantum, bensì come un processo continuo in cui le strategie e gli strumenti vengono progressivamente affinati, modificati o sostituiti in relazione al feedback ottenuto dalla loro applicazione.

Eventuali aggiornamenti successivi, anche infra-annuali, correlati agli esiti dei monitoraggi o alla sopravvenienza di nuove normative o prassi ovvero alla necessità di conformarsi a provvedimenti e/o pareri dell’autorità di controllo o del RPD, saranno oggetto di approvazione da parte dello stesso organo che ha approvato il PPD.

ATTORI INTERNI ALL'AMMINISTRAZIONE CHE HANNO PARTECIPATO ALLA PREDISPOSIZIONE DEL PIANO, NONCHÈ CANALI E STRUMENTI DI PARTECIPAZIONE

Oltre al titolare, hanno contribuito alla predisposizione del Piano, per quanto di propria competenza:

- dirigenti delegati al trattamento e, loro tramite, i soggetti autorizzati al trattamento (incaricati), in relazione, in particolare, alle proposte di svolgere una valutazione d'impatto sulla protezione dei dati, ai contributi alla valutazione d'impatto sulla protezione dei dati e al coinvolgimento nel processo di convalida di detta valutazione, figure individuate con Decreti del Presidente e Decreti/Determinazioni Dirigenziali del Direttore Generale/Dirigenti;

- responsabile della sicurezza dei sistemi informativi e responsabile IT, figura coincidente con quella del Direttore Generale;
- responsabile Protezione dei dati - RPD.

Nell'operazione di aggiornamento del Piano si tiene conto delle indicazioni fornite dallo staff del DPO nel corso delle teleconferenze periodiche e delle variazioni della dotazione organica intervenute negli ultimi mesi dell'anno 2024 e nei primi mesi dell'anno 2025. L'aggiornamento riguarda, pertanto, principalmente i contenuti di alcuni allegati del Piano, ma l'occasione è utile anche per effettuare un nuovo monitoraggio dei procedimenti già mappati e dei correlati trattamenti, anche in considerazione del monitoraggio già effettuato dagli uffici alla fine dell'anno 2024 sui procedimenti mappati. Non essendo comunque intervenute modifiche rilevanti nell'ambito dei procedimenti di competenza dell'Ente dal punto di vista dei dati trattati, non risulta necessario effettuate nuove valutazioni di impatto (DPIA). Al riguardo, come concordato nel corso delle teleconferenze periodiche con lo staff di supporto, si è stabilito di inoltrare al DPO apposito parere sulle DPIA compilate in piattaforma, seppur rappresentando l'assenza di modifiche sostanziali rispetto alle precedenti versioni. In data 10 aprile 2025 il DPO ha rilasciato parere favorevole, con la raccomandazione di procedere all'aggiornamento delle valutazioni di impatto in caso di cambiamenti rilevanti nei trattamenti o nelle misure adottate o in caso di data breach, o ancora nel caso di nuovi trattamenti che prevedono l'uso di nuove tecnologie con conseguente rischio elevato per i diritti e per le libertà delle persone fisiche.

CANALI, STRUMENTI E INIZIATIVE DI COMUNICAZIONE DEI CONTENUTI

Il Piano viene portato alla conoscenza dei dipendenti, dei collaboratori, della cittadinanza e dei soggetti a qualunque titolo coinvolti nell'attività dell'Ente mediante i seguenti strumenti:

- pubblicazione sul sito istituzionale a tempo indeterminato sino a revoca o sostituzione con un PPD aggiornato, nonché nella sezione "Amministrazione trasparente";
- invio a tutto il personale dipendente tramite rete intranet.

PARTE II

DATI PERSONALI, RISCHIO DI VIOLAZIONE E DISCIPLINA DEL GDPR

IL RISCHIO PER I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI E LA NEUTRALIZZAZIONE DEL RISCHIO ATTRAVERSO IL SISTEMA DI PROTEZIONE

Nell'attuale contesto, lo sviluppo e la rapidità dell'evoluzione tecnologica nonché la globalizzazione comportano nuove sfide per la protezione dei dati personali. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. Nel contempo, la tecnologia attuale consente a soggetti pubblici e privati di utilizzare dati personali come mai in precedenza, e la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati, tenuto conto dell'aumento del rischio di violazione dei dati medesimi e della necessità che le persone fisiche abbiano il controllo dei dati personali che li riguardano in un quadro di certezza giuridica e operativa rafforzata così come delineata del GDPR.

Il rischio inerente al trattamento è da intendersi come rischio di impatti negativi sulle libertà e sui diritti degli interessati, rispetto ai quali il titolare del trattamento è tenuto a promuovere e adottare approcci e politiche che tengano conto costantemente del rischio, effettuando un'analisi attraverso un apposito processo di valutazione (si vedano artt. 35-36 GDPR) che sappia tenere conto:

- dei rischi noti o evidenziabili;
- delle misure tecniche e organizzative adottate o che si intende adottare per mitigare il rischio.

A tal fine, il titolare del trattamento, attraverso il sistema di protezione, promuove e adotta approcci e politiche che tengano conto costantemente del rischio, prevedendo:

- l'obbligo di effettuare valutazioni di impatto (DPIA) prima di procedere ad un trattamento di dati che presenti rischi elevati per i diritti delle persone, e di consultare l'Autorità di protezione dei dati in caso di dubbi;
- adeguate misure di sicurezza;
- un sistema di monitoraggio sull'efficacia delle misure;
- la figura del "Responsabile della protezione dei dati" (RPD/DPO).

All'esito dell'analisi, condotta anche attraverso la valutazione di impatto (DPIA), il titolare del trattamento decide, in autonomia, se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale, fermo restando che l'autorità non ha il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e può, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58 GDPR (dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento).

L'EGAS tratta i dati personali necessari per lo svolgimento delle proprie finalità istituzionali, quali identificate da disposizioni di legge, statutarie e regolamentari, e nel rispetto dei limiti imposti dalla vigente normativa in materia di protezione dei dati personali e dai provvedimenti delle Autorità di controllo. Le operazioni di trattamento possono avvenire esclusivamente ad opera dei soggetti all'uopo delegati, designati ed autorizzati secondo quanto previsto nel presente documento. Non è consentito il trattamento da parte di persone non puntualmente autorizzate ed istruite in tal senso.

Nell'ambito delle operazioni di trattamento conseguenti all'esercizio delle proprie funzioni istituzionali l'Ente tratta le seguenti tipologie di dati:

- dati personali, quali definiti all'articolo 4, paragrafo 1 del GDPR;
- categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 del GDPR (c.d. dati sensibili);
- categorie particolari di dati personali di cui all'articolo 2-septies del D.Lgs. 196/2003 (c.d. dati super-sensibili);
- dati personali relativi a condanne penali e reati di cui all'articolo 10 del GDPR (c.d. dati giudiziari).

La mole di dati personali è ad ogni modo limitata in considerazione del fatto che l'EGAS non eroga servizi a domanda individuale.

L'ACCOUNTABILITY QUALE CONSEGUENZA DELL'APPROCCIO BASATO SUL RISCHIO

Nell'articolo 5 comma 2 del GDPR si rinviene il principio di "accountability" come criterio guida del Regolamento per la protezione dei dati personali. In italiano è stato tradotto con il termine "responsabilizzazione" ma il concetto non è chiaramente interpretabile solo come "responsabilità". Sarebbe molto limitativo e non pienamente conforme all'approccio voluto invece dal legislatore.

Nell'ambito della tutela e protezione dei dati personali il concetto di "accountability" assume un ruolo fondamentale, la chiave di lettura e di interpretazione sul giusto comportamento che il titolare del trattamento deve adottare da adottare davanti ad un quesito, ad un problema, al dubbio sul corretto processo organizzativo o tecnico alla base di un trattamento dei dati.

Responsabilizzare il titolare di un trattamento dati fa sì che quest'ultimo non sia più mero esecutore di un elenco di misure imposte ad una norma, ma divenga responsabile delle misure operative e tecniche che riterrà opportune, efficaci e dunque adeguate a salvaguardare i dati che tratta.

Il GDPR pone con forza l'accento sulla "responsabilizzazione" (accountability) del titolare e dei responsabili, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del GDPR.

Il principio di responsabilizzazione richiede che:

- il titolare ed i responsabili di trattamento istituiscano e tengano costantemente aggiornato, in forma scritta, anche elettronica, il registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30 GDPR, fermo restando che il titolare o un suo delegato può inserire ulteriori informazioni se lo ritiene opportuno, proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti. Il registro costituisce uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno dell'Ente, indispensabile per ogni valutazione e analisi del rischio;
- il titolare del trattamento, anche ai fini della istituzione e della tenuta del registro, compia e tenga costantemente aggiornata un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche;
- effettuata la ricognizione dei trattamenti, il titolare valuti l'adeguato livello di sicurezza da adottare, tenendo conto in particolare dei rischi che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati;
- in caso di violazione dei dati personali il titolare del trattamento notifichi la violazione all'autorità di controllo competente, secondo le modalità descritte nel corpo del presente provvedimento.

Anche la designazione di un "Responsabile della protezione dati" (RPD/DPO), quale figura indipendente, autorevole, dotata di competenze manageriali e tenuta al segreto d'ufficio, riflette l'approccio responsabilizzante che è proprio del GDPR, essendo finalizzata a facilitare l'adeguamento del GDPR da parte del titolare e del responsabile. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento nello svolgimento dei compiti affidati, specificati nel corpo del presente documento.

L'INFORMATIVA

Contenuti dell'informativa

I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del GDPR.

In particolare, il titolare deve sempre specificare:

- i dati di contatto del RPD-DPO ove esistente;
- la base giuridica del trattamento;
- il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento;
- se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti.

Il GDPR prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente". In particolare, il titolare deve specificare:

- il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
- il diritto di presentare un reclamo all'autorità di controllo.

Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Tempi dell'informativa

Nel caso di dati personali non raccolti direttamente presso l'interessato l'informativa deve essere fornita entro un termine ragionevole che non può superare un mese dalla raccolta, oppure al momento della comunicazione dei dati (a terzi o all'interessato).

Modalità dell'informativa

L'informativa deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile.

Occorre utilizzare un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee.

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi online, anche se sono ammessi "altri mezzi", potendo essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra.

Il GDPR ammette, soprattutto, l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa e conformemente ai modelli di icone definite prossimamente dalla Commissione europea.

In caso di dati personali raccolti da fonti diverse dall'interessato occorre valutare caso per caso se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato.

L'informativa deve essere fornita all'interessato prima di effettuare la raccolta dei dati.

Se i dati non sono raccolti direttamente presso l'interessato, l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento.

In tutti i casi, il titolare deve specificare:

- la propria identità;
- quella dell'eventuale rappresentante nel territorio italiano;
- le finalità del trattamento;
- i diritti degli interessati (compreso il diritto alla portabilità dei dati);
- se esiste un responsabile del trattamento e la sua identità;
- quali sono i destinatari dei dati.

Ogni volta che le finalità cambiano è necessario informarne l'interessato prima di procedere al trattamento ulteriore.

Il presente PPD tiene conto e recepisce le raccomandazioni del Garante, di seguito indicate:

- fermo restando che il GDPR supporta chiaramente il concetto di informativa "stratificata", più volte esplicitato dal Garante nei suoi provvedimenti in particolare attraverso l'impiego di icone associate (in vario modo) a contenuti più estesi, che devono essere facilmente accessibili, e promuove l'utilizzo di strumenti elettronici per garantire la massima diffusione e semplificare la prestazione delle informative, una volta adeguata l'informativa nei termini sopra indicati, i titolari potranno continuare o iniziare ad utilizzare queste modalità per la prestazione dell'informativa, comprese le icone che l'Autorità ha in questi anni suggerito nei suoi provvedimenti (videosorveglianza, banche, ecc.), in attesa della definizione di icone standardizzate da parte della Commissione;
- devono essere adottate misure organizzative interne idonee a garantire il rispetto della tempistica:
- il termine di un mese per l'informativa all'interessato è un termine massimo, e occorre ricordare che l'art. 14, paragrafo 3, lettera a), del GDPR menziona in primo luogo che il termine deve essere "ragionevole";

- poiché spetta al titolare valutare lo sforzo sproporzionato richiesto dall'informare una pluralità di interessati, qualora i dati non siano stati raccolti presso questi ultimi, e salva l'esistenza di specifiche disposizioni normative nei termini di cui all'art. 23, paragrafo 1, del GDPR, è utile fare riferimento ai criteri evidenziati nei provvedimenti con cui il Garante ha riconosciuto negli anni l'esistenza di tale sproporzione.

I DIRITTI DEGLI INTERESSATI

Trasparenza e modalità trasparenti per l'esercizio dei diritti dell'interessato sono alla base della disciplina del GDPR. In particolare, il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura tecnica e organizzativa a ciò idonea. Benché sia il solo titolare a dover dare riscontro in caso di esercizio dei diritti, il responsabile è tenuto a collaborare con il titolare o un suo delegato ai fini dell'esercizio dei diritti degli interessati.

Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3).

La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre ad utilizzare un linguaggio semplice e chiaro.

Diritto di accesso

Il presente PPD tiene conto della disciplina del GDPR in tema di diritto di accesso secondo la quale l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia di cui al paragrafo 3 dell'art. 15 GDPR non deve comunque ledere i diritti e le libertà altrui.

Diritto alla rettifica e cancellazione

Il presente PPD tiene conto della disciplina del GDPR in tema di diritto di rettifica e cancellazione ("diritto all'oblio"), di seguito indicata.

Quanto al diritto di rettifica, l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Quanto al diritto cosiddetto "all'oblio", l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

Il titolare, se ha reso pubblici dati personali ed è obbligato a cancellarli ai sensi del paragrafo 1, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;

b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;

d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;

e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Diritto alla limitazione

Il presente PPD tiene conto della disciplina del GDPR in tema di diritto alla limitazione, di seguito indicata.

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti condizioni:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 del GDPR, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali limitazioni del trattamento salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Diritto alla portabilità

Il presente PPD tiene conto della disciplina del GDPR in tema di diritto alla portabilità dei dati, di seguito indicata.

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati ad un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b);

b) il trattamento sia effettuato con mezzi automatizzati.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

L'esercizio del diritto alla portabilità lascia impregiudicato il diritto alla cancellazione. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Il diritto alla portabilità non deve ledere i diritti e le libertà altrui.

Diritto di opposizione e processo decisionale automatizzato relativo alle persone

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del GDPR, compresa la profilazione sulla base di tali disposizioni.

Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1 GDPR, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Il presente PPD tiene conto e recepisce le raccomandazioni del Garante, di seguito indicate.

- Modalità per l'esercizio dei diritti

È opportuno che il titolare di trattamento adotti le misure tecniche e organizzative eventualmente necessarie per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati, che dovrà avere per impostazione predefinita forma scritta (anche elettronica). Potranno risultare utili le indicazioni fornite dal Garante nel corso degli anni con riguardo all'intelligibilità del riscontro fornito agli interessati e alla completezza del riscontro stesso. Quanto alla definizione eventuale di un contributo spese da parte degli interessati, che il regolamento rimette al titolare del trattamento, va tenuto presente che l'Autorità intende valutare l'opportunità di definire linee-guida specifiche.

- Diritto di accesso

Oltre al rispetto delle prescrizioni relative alla modalità di esercizio di questo e degli altri diritti, il titolare può consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.

- Diritto alla limitazione

Il diritto alla limitazione prevede che il dato personale sia "contrassegnato" in attesa di determinazioni ulteriori; pertanto, è opportuno che il titolare preveda nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

- Diritto alla portabilità

Il diritto alla portabilità consente all'interessato di ricevere i dati personali forniti ad un titolare, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasmetterli ad un altro titolare del trattamento senza impedimenti.

Il Gruppo di lavoro "Articolo 29" ha pubblicato nel mese di dicembre 2016 linee-guida specifiche, emendate nel mese di aprile 2017, dove sono illustrati e spiegati i requisiti e le caratteristiche del diritto alla portabilità con particolare riguardo ai diritti di terzi interessati i cui dati siano potenzialmente compresi fra quelli "relativi all'interessato" di cui quest'ultimo chiede la portabilità.

Vanno inoltre tenuti presente i numerosi provvedimenti con cui l'Autorità ha indicato criteri per il bilanciamento fra i diritti e le libertà fondamentali di terzi e quelli degli interessati esercitanti i diritti.

Poiché la trasmissione dei dati da un titolare all'altro prevede che si utilizzino formati interoperabili, i titolari che ricadono nel campo di applicazione di questo diritto dovrebbero adottare da subito le misure necessarie a produrre i dati richiesti in un formato interoperabile.

PARTE III
CONTESTO, SOGGETTI RESPONSABILI, SICUREZZA E DOCUMENTAZIONE DEL SISTEMA DI PROTEZIONE

IL CONTESTO DEL SISTEMA DI PROTEZIONE

La descrizione riassuntiva del contesto ha lo scopo di delineare il complessivo stato di fatto e di diritto nel quale si inserisce il trattamento, sia con riferimento al contesto esterno che con riferimento al contesto interno.

Rileva in particolare il contesto interno, che tiene conto:

- degli atti di programmazione e pianificazione generale dell'Ente (disposizioni e atti generali, circolari, istruzioni), di organizzazione e articolazione degli uffici (organigramma e funzionigramma), della mappatura dell'attività (processi e procedimenti), dell'inventario dei beni (mobili e immobili) e della mappatura delle risorse strumentali, degli eventuali elenchi di consulenti e collaboratori, degli atti e dei provvedimenti degli organi di indirizzo e gestionali, del catalogo di dati, metadati, banche dati;
- dei soggetti che effettuano il trattamento e degli eventuali soggetti autorizzati ad accedere ai locali fuori dall'orario di servizio.

I SOGGETTI E LE RESPONSABILITÀ

Titolare del trattamento

Come riportato nelle definizioni, 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 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.

Dunque, il titolare è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo a cui competono, anche unitamente ad altro titolare, le decisioni in ordine:

- alle finalità;
- alle modalità del trattamento di dati personali;
- agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Conformemente alle disposizioni del GDPR, il titolare può designare, sotto la propria responsabilità, e all'interno del proprio assetto organizzativo, determinate persone fisiche per attribuire alle stesse specifici compiti e funzioni connessi al trattamento dei dati, individuando le modalità più opportune per autorizzare dette persone al trattamento dei dati. Le modalità più opportune a tal fine sono costituite dalla delega di compiti e funzioni alle persone fisiche designate, individuate nel Direttore Generale e nei Dirigenti dell'Ente.

Contitolari del trattamento

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento.

I contitolari determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, con particolare riguardo:

- all'esercizio dei diritti dell'interessato;

- alle rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 GDPR, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti.

Tale accordo deve designare un punto di contatto dei contitolari per gli interessati. L'accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato. Indipendentemente dalle disposizioni dell'accordo, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

Responsabili del trattamento e sub-responsabili

Il GDPR ha modificato la definizione di responsabile del trattamento in “persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento”.

Per effetto di tale modifica, il responsabile è il soggetto esterno alla struttura organizzativa che agisce "per conto del titolare".

Il responsabile è designato dal titolare facoltativamente. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti. In particolare, il titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincola il responsabile del trattamento al titolare del trattamento e che individua la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Il contratto o altro atto giuridico dettaglia, analiticamente, i compiti affidati al responsabile e prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32 del GDPR;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Con riguardo alla lettera h), il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente PPD o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Il responsabile effettua il trattamento attenendosi alle condizioni stabilite nel contratto o atto giuridico, e alle istruzioni impartite dal titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di legge e regolamento, delle proprie istruzioni e di quanto stabilito nel contratto o atto giuridico.

Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente PPD. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 del GDPR o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti.

Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui sopra può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 dell'articolo 28 del GDPR, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43 del GDPR.

Autorizzati al trattamento (incaricati)

Pur non prevedendo espressamente la figura dell'"incaricato" del trattamento (ex art. 30 Codice), il GDPR non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile".

Il D.Lgs. 101/2018, prevedendo l'introduzione, nel D.Lgs. 196/2003, dell'art. 2-quaterdecies, dispone che il titolare o il responsabile del trattamento possano prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

Raccomandazioni del Garante su titolare, responsabile e incaricato del trattamento

Il presente PPD tiene conto e recepisce le raccomandazioni del Garante sui fondamenti di liceità del trattamento, di seguito indicate.

I titolari del trattamento devono valutare attentamente l'esistenza di eventuali situazioni di contitolarità, essendo obbligati in tal caso a stipulare l'accordo interno di cui parla l'art. 26, paragrafo 1, del GDPR.

È necessario, in particolare, individuare il "punto di contatto per gli interessati" previsto dal suddetto articolo ai fini dell'esercizio dei diritti previsti dal GDPR.

Il titolare di trattamento deve verificare che i contratti o altri atti giuridici che attualmente disciplinano i rapporti con i rispettivi responsabili siano conformi a quanto previsto, in particolare, dall'art. 28, paragrafo 3, del GDPR. Devono essere apportate le necessarie integrazioni o modifiche entro il 25 maggio 2018, in particolare qualora si intendano designare sub-responsabili nei termini sopra descritti.

Attraverso l'adesione a codici deontologici ovvero l'adesione a schemi di certificazione il responsabile può dimostrare le "garanzie sufficienti" di cui all'art. 28, paragrafi 1 e 4 del GDPR.

Responsabile della protezione dei dati (RPD/DPO)

Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal GDPR.

Il Responsabile della protezione dei dati è incaricato dei seguenti compiti:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente GDPR nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del presente GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento 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;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del DGPR;
- cooperare con l'autorità di controllo;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti, il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Il Responsabile della protezione dei dati, inoltre:

- va tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
- va sostenuto nell'esecuzione dei propri compiti fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica;
- non deve ricevere alcuna istruzione per quanto riguarda l'esecuzione dei propri compiti.

Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

Il RPD/DPO:

- può svolgere altri compiti e funzioni a condizione che tali compiti e funzioni non diano adito a un conflitto di interessi;
- è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

LA SICUREZZA

Misure di sicurezza

Fermo restando il principio che qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali e che, salvo quanto previsto dalla legge per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato, i trattamenti in ambito pubblico devono svolgersi in modo lecito e garantendo la sicurezza. A tal fine, il GDPR stabilisce che il titolare del trattamento attui misure adeguate a garantire ed essere in grado di dimostrare il rispetto di detto GDPR, tenendo conto tra l'altro dei "rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche" (articolo 24, paragrafo 1). L'obbligo per il titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati va inteso nel contesto dell'obbligo generale, cui gli stessi sono soggetti, di gestire adeguatamente i rischi.

Tenendo conto dello stato dell'arte e dei costi di adeguamento, 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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in particolare dei rischi presentati dal trattamento che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

L'adesione a un codice di condotta approvato di cui all'articolo 40 del GDPR o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Codici di condotta

Il presente PPD tiene conto che gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente GDPR, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

Per i codici di condotta si rinvia ai codici approvati dal Garante e al DPR n. 62/2013 nonché al codice di comportamento approvato dal Titolare ad integrazione del citato DPR n. 62/2013.

Certificazione

Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente GDPR dei trattamenti effettuati dal titolare del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese.

La certificazione è volontaria e accessibile tramite una procedura trasparente.

La certificazione ai sensi dell'art. 42 del GDPR non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al GDPR e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti.

La certificazione ai sensi dell'art. 42 del GDPR è rilasciata dagli organismi di certificazione di cui all'articolo 43 del GDPR o dall'autorità di controllo competente.

Il titolare del trattamento o il responsabile del trattamento che sottopone il trattamento effettuato al meccanismo di certificazione fornisce all'organismo di certificazione di cui all'articolo 43 del GDPR o, ove applicabile, all'autorità di controllo competente tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione.

La certificazione è rilasciata al titolare del trattamento o responsabile del trattamento per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti. La certificazione è revocata, se del caso, dagli organismi di certificazione di cui all'articolo 43 del GDPR o dall'autorità di controllo competente, a seconda dei casi, qualora non siano o non siano più soddisfatti i requisiti per la certificazione.

Notifica di una violazione dei dati personali all'Autorità di controllo

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 del GDPR senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

La notifica deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Per le notifiche all'Autorità di controllo, il presente PPD rinvia alla “procedura per la gestione di data breach ai sensi del GDPR (Regolamento europeo 679/2016) allegato al “Regolamento sulla protezione dei dati personali” approvato con deliberazione del CIA n. 15 del 15 aprile 2020.

Comunicazione di una violazione dei dati personali all'interessato

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

La comunicazione all'interessato descrive, con un linguaggio semplice e chiaro, la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d) del GDPR:

- comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni sopra citate è soddisfatta.

Per la comunicazione di una violazione dei dati personali all'interessato, il presente PPD rinvia alla “procedura per la gestione di data breach ai sensi del GDPR (Regolamento europeo 679/2016) allegato al “Regolamento sulla protezione dei dati personali” approvato con deliberazione del CIA n. 15 del 15 aprile 2020.

La documentazione

Le diverse componenti del sistema di protezione, come dettagliate nel corpo del presente Piano, sono documentate, oltre dal Piano stesso, almeno da:

- Registri delle attività e delle categorie dei trattamenti;
- Mappe della struttura organizzativa e dei soggetti;
- Schede di ricognizione dei trattamenti/Elenco dei trattamenti;
- Schede di determinazione preliminare della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del GDPR (UE) 2016/679/ Schede di assoggettabilità a DPIA;
- Mappa dei luoghi;

- Mappe di hardware, software, archivi e banche dati;
- Mappa dei rischi e delle motivazioni di stima;
- Mappa delle misure di sicurezza logistiche/fisiche;
- Mappa delle misure di sicurezza informatiche/logiche;
- Mappa delle misure di sicurezza organizzative;
- Mappa delle misure di sicurezza e procedurali;
- Elenco delle misure di sicurezza correlate all'indice dei trattamenti e suddivise per uffici;
- Corsi di formazione.

PARTE IV
GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000

Principi applicabili alla gestione del rischio

La gestione del rischio diventa lo strumento atto a dimostrare l'adeguatezza delle misure implementate a tutela dei dati trattati.

Sulla base della Norma UNI ISO 31.000, e ai fini della strategia di protezione dei dati personali, viene definita:

- la nozione di "rischio" come uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità;
- la nozione di "gestione dei rischi" come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.

La gestione di rischi derivanti dal trattamento sulla protezione dei dati personali viene condotta tenendo presente i principi contenuti nella Norma UNI ISO 31.000 e viene condotta attraverso le fasi di:

- analisi del rischio, quale fase del processo di gestione nella quale viene definito il contesto esterno e interno, di natura organizzativa e gestionale;
- valutazione del rischio, quale fase del processo di gestione del rischio che identifica, analizza e pondera il rischio medesimo;
- trattamento del rischio.

GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000: FASE DELLA ANALISI

I documenti allegati e, in particolare, la ricognizione dei trattamenti in rapporto a tutta l'attività dell'ente, le schede di DPIA e l'elenco dei rischi, della gravità rilevata dalla prospettiva degli interessati e della relativa motivazione, comprovano l'effettuazione della analisi dei rischi derivanti dai trattamenti, e l'accuratezza della analisi medesima.

Contesto interno organizzativo

Struttura organizzativa – soggetti delegati e autorizzati

La struttura organizzativa dell'Ente è indicata nella mappa della struttura organizzativa allegata, e corrisponde alle funzioni istituzionali ed ai compiti assegnati a ciascuna struttura.

L'elenco dei soggetti interni, allegata al presente documento, riepiloga i dati dei dirigenti delegati dal titolare e dei soggetti incaricati. Come riportato in precedenza, nel corso del 2021 era stato effettuato un aggiornamento in merito ai soggetti delegati al trattamento, in considerazione dell'assunzione a tempo determinato di n. 1 Dirigente a partire dal mese di maggio 2021. Era stato pertanto predisposto un nuovo decreto presidenziale (n. 5 del 26 maggio 2021), che aveva aggiornato i contenuti del Decreto n. 1/2020 con

l'attribuzione di nuove deleghe al suddetto Dirigente. Si era conseguentemente proceduto all'aggiornamento dei relativi dati nell'apposita sezione presente sul sito internet dell'Ente.

In considerazione della cessazione per dimissioni del suddetto Dirigente, e dell'assunzione, a partire dal 1 maggio 2023, di un nuovo Dirigente amministrativo ai sensi dell'art. 110 del Tuel, analoga attività è stata svolta nell'anno 2023. Con Decreto n. 4 dell'8 giugno 2023 si è, dunque, proceduto, all'attribuzione di nuove deleghe al soggetto neo-assunto.

Ciò premesso, si indicano i soggetti designati dal titolare per lo svolgimento di specifici compiti e funzioni in ordine al trattamento dei dati:

- soggetti che operano sotto la diretta autorità del titolare ai quali sono stati attribuiti e delegati specifici compiti e funzioni connessi al trattamento di dati personali, relativi ai trattamenti rientranti nella struttura organizzativa di competenza (Decreto del Presidente n. 1 del 8 aprile 2020, di aggiornamento del Decreto del Presidente n. 12 dell'8 novembre 2018, n. 5 del 26 maggio 2021, di aggiornamento del precedente in considerazione dell'assunzione a tempo determinato di n. 1 Dirigente amministrativo a partire dal mese di maggio 2021, e n. 4 del'8 giugno 2023, con cui si è preso atto dell'assunzione a tempo determinato di un nuovo Dirigente amministrativo dal mese di maggio 2023):
    - Direttore Generale (Area Direzione Generale)
    - Dirigente dell'Area Amministrazione e Finanze;
    - Dirigente dell'Area Pianificazione, Programmazione e Controllo;
- dipendenti che operano nella struttura organizzativa di competenza, e sotto la diretta autorità del titolare, per il trattamento dei dati personali, ai quali sono stati attribuiti specifici compiti e funzioni ed ai quali è stata conferita formale autorizzazione a trattare dati personali conformemente al GDPR, alla normativa interna di adeguamento, alle Linee guida delle Autorità di controllo, alle specifiche istruzioni sulle modalità a cui attenersi nel trattamento indicate nel presente atto e, infine, alle eventuali indicazioni del RPD/PDO (Decreto del Direttore Generale n. 1 del 9 aprile 2020, di parziale conferma del Decreto del Direttore Generale n. 2 del 14 novembre 2018; Decreto del Direttore Generale n. 3 del 21 luglio 2021; Determinazione del Dirigente APPCG n. 144 del 23 luglio 2021; Determinazione del Dirigente AAF n. 141 del 21 luglio 2021, Decreto del Direttore Generale n. 2 del 29 aprile 2022; Determinazione del Dirigente AAF n. 154 del 29 aprile 2022; Determinazione del Dirigente APPCG n. 150 del 16 giugno 2023, Decreto del Direttore Generale n. 2 del 20 dicembre 2023, Determinazioni del Dirigente AAF n. 294 del 28 dicembre 2023 e n. 71 dell'11 aprile 2025):
- Referente per le attività connesse alle funzioni RDP e di contatto con l'RDP (Decreto del Direttore Generale n. 1 del 9 aprile 2020, di conferma del Decreto del Direttore Generale n. 2 del 14 novembre 2018):

Soggetti: Contitolari del trattamento e titolari autonomi

Dagli allegati relativi ai soggetti si rileva l'assenza di contitolari del trattamento.

Il titolare autonomo del trattamento è una figura non citata dal GDPR, eppure presente nei fatti. Il suddetto termine viene utilizzato quando, in presenza di un primo titolare, un soggetto diverso a cui legittimamente sono trasferiti i dati, processa gli stessi per finalità distinte rispetto a quelle del titolare, assumendo così a sua volta una funzione distinta di titolare, che può presentarsi in concomitanza ad un ruolo di responsabile del trattamento, o meno. Tale ipotesi si differenzia nettamente da quella per cui due o più soggetti concorrono a definire una o più finalità comuni, che è il caso della sopra citata contitolarità.

Si rileva inoltre la presenza di alcuni titolari autonomi, individuati nel medico competente, nei soggetti che gestiscono le assicurazioni contratte dall'Ente e nei componenti del Collegio dei Revisori.

Soggetti: Responsabili del trattamento e sub-responsabili

Nell'allegato riferito ai responsabili esterni sono indicati i casi in cui un trattamento debba essere effettuato, per conto del titolare del trattamento, da un responsabile del trattamento che presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.

I trattamenti da parte di un responsabile del trattamento esterno sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Spetta ai Dirigenti identificare i responsabili e gli eventuali sub responsabili di riferimento della struttura organizzativa di competenza, e sottoscrivere i contratti/appendici contrattuali per il trattamento dei dati.

Soggetti: Responsabile della protezione dati (RPD/DPO)

In merito alla designazione del RPD si richiamano i seguenti atti:

- il Decreto del Presidente n. 9 del 4 luglio 2018 con cui è stato designato l'avv.to Nadia Corà quale Responsabile della protezione dei dati personali (RPD) per l'Ente di Governo dell'Ambito della Sardegna, in forza della stipulazione del contratto di servizio della durata di un anno con la persona giuridica Soluzione s.r.l. (Determinazione Dirigenziale n. 121 del 25 giugno 2018);
- la Determinazione Dirigenziale n. 131 del 14 giugno 2019 con la quale, in virtù dell'affidamento alla società Soluzione s.r.l. del servizio di adeguamento agli obblighi previsti nel Regolamento UE 2016/679 per la durata di tre anni, è stato confermato l'affidamento dell'incarico di Responsabile della protezione dei dati personali (RPD) per l'Ente di Governo dell'Ambito della Sardegna all'avv.to Nadia Corà;
- la Determinazione Dirigenziale n. 214 del 23 giugno 2022, con la quale, in virtù dell'affidamento alla società Maggioli SpA del servizio di adeguamento agli obblighi previsti nel Regolamento UE 2016/679 per la durata di tre anni, è stato confermato l'affidamento dell'incarico di Responsabile della protezione dei dati all'avv.to Nadia Corà;
- il Decreto del Presidente n. 3 dell'8 giugno 2023, con il quale, a seguito di comunicazione del RPD, si è preso atto dei nuovi dati di contatto dello stesso, stabilendo di designare, per la durata del contratto di servizio stipulato con Maggioli SpA, Rete Entionline All Privacy, costituita dalla persona giuridica Gruppo Maggioli S.p.A e dall'Avv.to Nadia Corà, quale Responsabile della protezione dei dati personali (RPD) per l'Ente di Governo dell'Ambito del Territorio della Sardegna e l'Avv.to Nadia Corà quale professionista referente della Rete Entionline All Privacy per l'Ente medesimo;
- la Determinazione Dirigenziale n. 136 del 26 giugno 2025, con la quale, in virtù dell'affidamento alla società Maggioli SpA del servizio di adeguamento agli obblighi previsti nel Regolamento UE 2016/679 per la durata di tre anni, è stato conferito l'incarico di Responsabile della protezione dei dati all'avv.to Guido Paratico;
- il Decreto del Presidente n. 3 luglio 2025, con il quale si è stabilito di designare, per la durata del contratto di servizio stipulato con Maggioli SpA, Rete Entionline All Privacy, costituita dalla persona giuridica Gruppo Maggioli S.p.A e dall'Avv.to Guido Paratico, quale Responsabile della protezione dei dati personali (RPD) per l'Ente di Governo dell'Ambito del Territorio della Sardegna e l'Avv.to Guido Paratico quale professionista referente della Rete Entionline All Privacy per l'Ente medesimo.

Di seguito si riportano, infine, i dati di Contatto:

Responsabile della Protezione dei Dati - RPD:

Denominazione: Rete Entionline All Privacy

P. IVA: 02066400405

Stato: Italia

Provincia: Brescia

Comune: Brescia, CAP 25136

Indirizzo: Via Triumplina, 183/B

Telefono: 0302531939

E-mail: consulenza@entionline.it

PEC: guido.paratico@mantova.pecavvocati.it

Soggetto individuato quale referente per il Titolare/Responsabile:

Cognome: Paratico

Nome: Guido

Dati di Contatto:

Telefono: 0376.1577119

Cellulare: 3397305252

E-mail: consulenza@entionline.it

PEC: guido.paratico@mantova.pecavvocati.it

Con riferimento alla prescrizione del Responsabile di programmare la digitalizzazione del Servizio Protezione dati personali (DPO), consentendo all'interessato del trattamento di presentare on-line un'istanza al Titolare, anche tramite il RPD, e dunque prevedendo un form on line, previa autenticazione con SPID o CIE, si conferma il rinvio alla futura predisposizione degli atti di programmazione finanziaria al fine di valutare la sussistenza di risorse finanziarie da dedicare all'eventuale attivazione del servizio. Tali valutazioni terranno conto del fatto che l'obbligo della digitalizzazione dei servizi della P.A., previsto dal D.L.76/2020 (convertito con L.120/2020), riguarda, in generale, tutti i servizi pubblici e non singoli servizi (come, ad esempio, i servizi alla persona e i servizi ambientali), non sussistendo, dunque, un obbligo specifico per il servizio DPO, che costituisce tuttavia un servizio rivolto a tutte le persone fisiche interessate dal trattamento dei loro dati personali da parte delle P.A.

È garantita, ad ogni modo, la possibilità, per gli interessati, di poter comunicare con il DPO o il Titolare, tramite posta elettronica ordinaria, il cui indirizzo è pubblicato sul sito dell'Ente.

Relativamente ai compiti del RPD, si rinvia a quanto sopra esposto.

Contesto interno gestionale e operativo

Schede di ricognizione dei trattamenti

Fanno parte del sistema di protezione le Schede di ricognizione dei trattamenti elaborate con riferimento a tutta l'attività svolta dall'Ente, prendendo in considerazione tutti i processi, inclusi i procedimenti amministrativi. Nello specifico, come di seguito maggiormente dettagliato, sono presenti l'elenco di assoggettabilità dei trattamenti a DPIA, con indicazione dei trattamenti sottoposti e dei trattamenti non sottoposti a DPIA, le schede contenenti la valutazione di impatto e l'elenco delle schede di sintesi DPIA, distinte per Aree o relative a trattamenti trasversali riguardanti tutti gli uffici.

Nel corso dell'aggiornamento del Piano è stato attuato un nuovo monitoraggio dei trattamenti correlati ai procedimenti, anche in considerazione del monitoraggio già effettuato dagli uffici alla fine dell'anno 2024 sui

procedimenti mappati. Di conseguenza viene effettuata, in caso di modifiche, una rivisitazione della determinazione della possibilità che i vari trattamenti possano presentare un rischio elevato ai fini del regolamento 2016/679 e delle conseguenti valutazioni di impatto (DPIA), con l'obiettivo di garantire un miglioramento costante delle misure già previste e/o in adozione. Come riportato in precedenza, non essendo intervenute modifiche rilevanti nell'ambito dei procedimenti di competenza dell'Ente dal punto di vista dei dati trattati, non risulta necessario effettuate nuove valutazioni di impatto (DPIA).

Mappa dei luoghi

La mappa dei luoghi, allegata al presente documento per formarne parte integrante e sostanziale, identifica i locali nei quali viene svolta l'attività lavorativa e, dunque, il possibile trattamento dei dati, con indicazione delle caratteristiche degli stessi, con particolare riferimento alle modalità di accesso ed agli eventuali sistemi di allarme/antincendio.

Mappa hardware, software, archivi e banche dati elettroniche

Le mappe, allegate al presente documento per formarne parte integrante e sostanziale, identifica:

- gli strumenti, i server e i locali di ubicazione, unitamente alla descrizione delle caratteristiche tecniche degli strumenti elettronici medesimi;
- i software in relazione agli archivi/banche dati che vengono gestiti dai software medesimi, unitamente ai soggetti abilitati all'accesso.

Nel corso della redazione del presente documento si è tenuto conto di alcune modifiche relative alla dotazione organica (nuove assunzioni, trasferimenti, cessazioni). Si è così proceduto all'aggiornamento delle mappe degli hardware e dei software, mentre resta invariata la mappa dei luoghi già aggiornata nel corso del 2022.

In considerazione della prevista scadenza al 31 luglio 2025 del contratto di locazione attualmente in essere, risulta in corso l'attività di ricerca di un nuovo immobile in locazione. Individuata una nuova sede, saranno prontamente aggiornate le mappe dei luoghi e dei beni informatici, che confluiranno nel prossimo Piano 2026/2028.

Contesto esterno: trattamenti effettuati da responsabili esterni e titolati autonomi

Come già indicato in precedenza, l'Elenco dei trattamenti effettuati da responsabili esterni e titolari autonomi, e allegato al presente documento per formarne parte integrante sostanziale, consente di rilevare il rischio derivante dai trattamenti effettuati nel contesto esterno alla struttura organizzativa del titolare.

PARTE V
GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000: FASE DELLA VALUTAZIONE

Determinazione di assoggettabilità dei trattamenti a valutazione di impatto - DPIA

In base alla Norma UNI ISO 31.000, la valutazione del rischio richiede l'identificazione, l'analisi e la ponderazione del rischio medesimo.

Ai fini della valutazione del rischio, il GDPR introduce l'obbligo di valutazione d'impatto del trattamento sulla protezione dei dati.

Una valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle

persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.

Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del GDPR.

L'azione preliminare da svolgere per la valutazione di impatto è la determinazione del titolare in ordine alla possibilità che il trattamento possa determinare un rischio elevato per i diritti e le libertà degli interessati, la cosiddetta "determinazione di assoggettabilità dei trattamenti a valutazione di impatto" (DPIA).

La decisione in ordine alla possibilità che il trattamento in epigrafe indicato possa produrre un rischio elevato sulla protezione dei dati delle persone fisiche e, quindi, sulla obbligatorietà della DPIA viene adottata applicando i 3 casi indicati dall'art. 35, paragrafo 3 del GDPR e i 9 criteri esplicativi contenuti nelle sopra citate Linee guida.

Nell'applicare i suddetti criteri si deve tenere conto di quanto segue:

- la DPIA è sempre obbligatoria, indipendentemente dalla presenza di uno o più criteri sopra menzionati, per tutti i trattamenti inclusi nell'elenco predisposto e pubblicato dall'Autorità di controllo ai sensi dell'art. 35, paragrafo 4 GDPR;
- la DPIA è sempre obbligatoria per i trattamenti inclusi nell'indice dei trattamenti dei dati sensibili e giudiziari ai sensi del Regolamento sul trattamento dei dati sensibili e giudiziari approvato dall'Ente conformemente allo schema tipo del Garante;
- fermo restando che, secondo le Linee guida, un trattamento che soddisfa 2 criteri deve formare oggetto di una valutazione d'impatto sulla protezione dei dati, tuttavia, al fine di garantire una maggiore garanzia di tutela, la ricorrenza anche di 1 solo criterio costituisce elemento sufficiente per originare l'obbligo di svolgimento della DPIA;
- maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati;
- se, pur applicando i criteri sopra indicati, la necessità di una DPIA non emerge con chiarezza, va comunque ritenuto sussistente l'obbligo di farvi ricorso in quanto la DPIA contribuisce all'osservanza delle norme in materia di protezione dati da parte dei titolari di trattamento;
- la valutazione d'impatto sulla protezione dei dati non è richiesta nei seguenti casi:
    - quando, sulla base di predetti criteri, risulta che il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche ";
    - quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo;
    - quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate;
    - qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e) del GPDR, trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10 GPDR).

In ordine ai diversi trattamenti, le schede allegate per formare parte integrante e sostanziale del presente PPD, evidenziano le determinazioni assunte, tenendo conto delle linee guida adottate in materia.

In base alle determinazioni di assoggettabilità a valutazione di impatto di cui alle allegate schede (DPIA-FASE 1), i trattamenti per i quali risulta determinato, sulla base dei criteri delle citate Linee guida, un elevato rischio per i diritti e le libertà delle persone fisiche, e che non rientrano tra le eccezioni per le quali non è obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del GDPR, sono assoggettati a valutazione di impatto (DPIA-FASE 2).

Laddove una valutazione d'impatto sulla protezione dei dati riveli la presenza di rischi residui elevati, il titolare o un suo delegato sarà tenuto a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento (articolo 36, paragrafo 1 GDPR). In tale contesto, la valutazione d'impatto sulla protezione dei dati deve essere fornita completa e non in forma sintetica (articolo 36, paragrafo 3, lettera e GDPR).

Nei casi in cui, invece, il titolare del trattamento non riesca a trattare in maniera sufficiente i rischi individuati (ossia i rischi residui rimangono elevati), dovrà essere consultata l'autorità di controllo.

Occorre tuttavia sottolineare che, indipendentemente dal fatto che la consultazione dell'autorità di controllo sia richiesta o meno in base al livello di rischio residuo, sussistono comunque gli obblighi di conservare una registrazione della valutazione d'impatto sulla protezione dei dati e di aggiornamento di detta valutazione al momento opportuno.

Nel corso dell'elaborazione del presente documento, come detto, non si è ravvisata la necessità di procedere ad una nuova determinazione della possibilità che i vari trattamenti possano presentare un rischio elevato ai fini del regolamento 2016/679 e le conseguenti valutazioni di impatto, Nonostante l'assenza di variazioni sostanziali nella determinazione dei trattamenti da valutare, a seguito di consultazione con lo staff del DPO si è ritenuto necessario formulare una richiesta di parere al DPO in merito alle DPIA presenti in piattaforma. In data 10 aprile 2025 il DPO ha rilasciato parere favorevole, con la raccomandazione di procedere all'aggiornamento delle valutazioni di impatto in caso di cambiamenti rilevanti nei trattamenti o nelle misure adottate o in caso di data breach, o ancora nel caso di nuovi trattamenti che prevedono l'uso di nuove tecnologie con conseguente rischio elevato per i diritti e per le libertà delle persone fisiche. Anche in occasione del presente aggiornamento, inoltre, il Piano sarà comunque trasmesso al DPO per opportuna conoscenza.

Fanno dunque parte del sistema di protezione:

- **Schede di ricognizione e elenco dei trattamenti, con determinazione preliminare della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del GDPR (UE) 2016/679**
- **Schede di valutazione di impatto sulla protezione dei dati (DPIA)**

PARTE VI
GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000: FASE DEL TRATTAMENTO

Misure di sicurezza del trattamento

Il GDPR prevede che il titolare del trattamento attui misure adeguate a garantire ed essere in grado di dimostrare il rispetto di detto GDPR, tenendo conto tra l'altro dei "rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche" (articolo 24, paragrafo 1). L'obbligo per il titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati va inteso nel contesto dell'obbligo generale, cui gli stessi sono soggetti, di gestire adeguatamente i rischi.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in particolare dei rischi presentati dal trattamento che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Mappa dei rischi e motivazioni di stima

La Mappa dei rischi, allegata al presente documento per formarne parte integrante sostanziale, costituisce un elenco dei principali eventi rischiosi che possono determinare la violazione dei dati e rileva, dalla prospettiva degli interessati, la gravità e la correlata motivazione.

Misure di sicurezza logistiche

Sicurezza di aree e locali: l'identificazione delle misure di sicurezza tecniche/logistiche deve tenere conto almeno dei sottoindicati elementi di rischio, indicati a titolo esemplificativo e non esaustivo:

a) Collocazione:

- Aziende vicine con lavorazioni pericolose;
- Installazioni vicine pericolose (aeroporti, depositi carburanti...);

b) Vicinanza servizi:

- Carabinieri o altre forze di polizia e vigilanza;
- Ospedali o altri presidi;
- Vigili del fuoco;

c) Misure presenti anti-intrusione:

- Antifurto;
- Vigilanza;
- Videosorveglianza;
- Controllo accessi;
- Recinzioni;
- Cancelli;

d) Misure presenti antincendio:

- Estintori;
- Idranti;
- Rilevatori;

e) Misure presenti per la regolarità degli impianti:

- Elettrico;
- Climatizzazione;
- Riscaldamento;

f) Misure presenti per la continuità elettrica:

- UPS;
- Generatori;

g) Procedure:

- Procedura di gestione degli accessi;
- Procedura di gestione dei visitatori/manutentori.

L'identificazione delle misure di sicurezza tecniche/logistiche prende in considerazione almeno le principali sottoindicate misure, elencate a titolo esemplificativo e non esaustivo:

a) Antifurto

- Sensori;
- Allarmi;
- Porta normale;
- Porta blindata;
- Serratura di sicurezza;
- Finestre con grate;
- Finestre senza grate;

b) Antincendio:

- Sensori;
- Allarmi;
- Estintori/Impianto antincendio;
- Impianti a norma;
- Porta taglia fuoco;
- Porta antincendio per fuga;
- Utilizzo materiale ignifugo;

c) Sicurezza ambientale:

- Piano di emergenza per la gestione dei rischi individuati;

d) Sicurezza accessi:

- Controllo;
- Registrazione;
- Altro;

e) Sicurezza CED:

- Adeguato posizionamento all'interno dell'edificio;
- Adeguate pareti soffitto/pavimento;
- Misure antieffrazione;
- Controllo accessi;
- Impianto di climatizzazione;
- Misure antincendio idonee all'uso con le apparecchiature presenti;
- Porte antincendio di adeguata dimensione;
- Rilevatori di fumo, calore, allagamento;

f) continuità operativa:

- Gruppo di continuità;

- Gruppo elettrogeno;
- Corretto ed ordinato posizionamento dei cavi elettrici;
- Corretto ed ordinato posizionamento dei cavi di rete;
- Posizionamento ordinato delle apparecchiature nei rack;
- Spazio intorno ai rack adeguato alla movimentazione e manutenzione delle apparecchiature;

g) Sistema di custodia archivi cartacei:

- Armadi blindati;
- Armadi ignifughi con serratura;
- Armadi ignifughi senza serratura;
- Altri armadi con serratura;
- Altri armadi senza serratura;
- Classificatori/cassetti con serratura;
- Classificatori/cassetti senza serratura;
- Cassaforte;
- Scaffalature;

Come prescritto dal DPO in sede di parere rilasciato in merito alle DPIA condotte nell'anno 2021, le misure di sicurezza di tipo logistico sono state individuate tenendo conto dell'importanza di:

- garantire la continuità dell'alimentazione elettrica in caso di incidente;
- custodire faldoni/schede/cartelle contenenti dati personali con la massima attenzione (es. armadi con serratura/cassaforte), garantendone l'accesso solo al personale preposto, autorizzato e designato al trattamento;
- garantire il miglioramento continuo delle misure già in adozione.

La mappa delle misure di sicurezza logistiche applicate ai diversi trattamenti, allegata al presente PPD per formarne parte integrante e sostanziale, documenta e comprova l'osservanza del GDPR.

Al riguardo si osserva che anche nell'anno corrente, per tutte le tipologie di misure, è stata effettuata un'analisi delle stesse in base alla loro avvenuta attuazione, completa o parziale, o mancata attuazione e alle relative cause. Sono state mantenute le misure attuate, anche parzialmente, e quelle da attuare nel periodo di vigenza del presente Piano.

Misure di sicurezza informatiche

Al fine di indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottate per contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi, ed in adeguamento della Direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri che emana disposizioni finalizzate a consolidare lo stato della sicurezza informatica nazionale, AgID ha provveduto ad emanare l'elenco ufficiale delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni".

Con l'avvenuta pubblicazione in Gazzetta Ufficiale (Serie Generale n.103 del 5-5-2017) della Circolare 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei ministri 1 agosto 2015)", le misure minime sono divenute di obbligatoria adozione per tutte le Amministrazioni.

Le Misure, che si articolano sull'adeguamento di controlli di natura tecnologica, organizzativa e procedurale, prevedono tre livelli di adeguamento. Il livello minimo è quello al quale ogni pubblica amministrazione,

indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme. I livelli successivi (standard e avanzato) rappresentano situazioni evolutive in grado di fornire livelli di protezione più completi, e dovrebbero essere adottati fin da subito dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visti come obiettivi di miglioramento da parte di tutte le altre organizzazioni.

L'Ente adotta le misure minime di sicurezza ICT. Si sottolinea che anche nell'ambito del Manuale di gestione documentale adottato dall'Ente, il Responsabile della gestione documentale ha predisposto il Piano di sicurezza del sistema di gestione informatica dei documenti, contenente opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali ai sensi dell'art. 32 del GDPR, anche in funzione della tipologia dei dati trattati. Sul suddetto Piano, che contiene la descrizione delle misure adottate e le modalità di implementazione delle stesse, è stato acquisito il parere del Responsabile della Protezione dei dati personali.

La mappa delle misure delle misure di sicurezza informatiche applicate ai diversi trattamenti inclusi i criteri e modalità di salvataggio e di ripristino della disponibilità dei dati, allegata al presente PPD per formarne parte integrante e sostanziale, documenta e comprova l'osservanza del GDPR.

Per l'analisi effettuata nell'anno corrente sull'applicabilità e sull'attuazione delle misure si rinvia a quanto esposto nel punto precedente.

Misure di sicurezza organizzative

A titolo esemplificativo e non esaustivo, si elencano:

- work flow: in applicazione dei principi della norma uni iso 31000, integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti;
- work flow: integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento;
- esercizio diritti: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità e la completezza del riscontro fornito agli interessati;
- formazione: formazione di tutti i soggetti che trattano dati personali sotto l'autorità del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'unione o degli stati membri;
- gestione dati: adeguate modalità di utilizzazione documenti;
- gestione dati: distruzione dei documenti non necessari;
- gestione dati: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonché necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del garante;
- informazione: informazione continua e aggiornamento costante su procedure operative e istruzioni;
- gestione privacy: analisi dei rischi e formazione professionale;

Si sottolinea, in merito all'individuazione delle prescrizioni organizzative, che in sede di parere rilasciato in merito alle DPIA condotte nell'anno 2021 il DPO ha voluto rimarcare il valore delle seguenti misure:

- formazione continua dei dipendenti;
- analisi dei rischi;
- verifica periodica del trattamento dei dati personali consentito ai singoli incaricati o alle unità organizzative;

- monitoraggio delle misure di protezione adottate per valutare l'efficienza delle stesse e l'eventuale implementazione;
- adozione di procedure operative/istruzioni/linee guida/mansionari per il trattamento dei dati;
- distruzione di documenti cartacei e informatici non necessari;
- tenuta di un registro per le richieste di consultazione dei dati;
- rispetto delle prescrizioni dell'Autorità Garante nell'attività di videosorveglianza.

Al riguardo, si conferma che, allo stato attuale, non è presente un registro per le richieste di consultazione dei dati, non avendo mai acquisito istanze di tal genere, e che nell'Ente non viene svolta alcuna attività di videosorveglianza.

La mappa completa delle misure delle misure di sicurezza organizzative, applicate ai diversi trattamenti allegata al presente PPD per formarne parte integrante e sostanziale, documenta e comprova l'osservanza del GDPR, con le stesse osservazioni effettuate ai punti precedenti.

Misure di sicurezza procedurali

A titolo esemplificativo e non esaustivo, si elencano:

- definizione e attuazione della procedura operativa per favorire l'esercizio dei diritti ed il riscontro alle richieste presentate dagli interessati;
- definizione e attuazione della procedura operativa per documentare e gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante;
- definizione e attuazione della procedura operativa per il tempestivo ripristino della disponibilità e dell'accesso dei dati personali in caso di incidente fisico o tecnico;
- definizione e attuazione della procedura operativa per la gestione delle credenziali di autenticazione;
- definizione e attuazione della procedura operativa per selezionare e formare i soggetti da inserire nel Piano formativo.

Si precisa, al riguardo, che il DPO ha rappresentato l'opportunità di adottare apposite procedure organizzative per:

- pseudonimizzazione e cifratura dei dati personali;
- ripristino tempestivo della disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- gestione delle credenziali di autenticazione.

In merito alla pseudonimizzazione si intende precisare che già con il Regolamento sulla protezione dei dati personali approvato con la deliberazione del CIA n. 15 del 15 aprile 2020, era stato stabilito, in particolare all'art. 18, che laddove documenti, dati e informazioni, oggetto di pubblicazione obbligatoria per finalità di trasparenza, contengano dati personali (codice fiscale, luogo e data di nascita, residenza, IBAN), questi ultimi devono essere oscurati, tranne deroghe previste da specifiche disposizioni. Gli stessi potranno essere indicati in appositi allegati ai documenti, che non saranno oggetto di pubblicazione. Analoga disciplina dovrà essere seguita in caso di effettuazione di verifiche sui requisiti per partecipare ad una procedura di appalto: nelle determinazioni dirigenziali di aggiudicazione si dovrà fare riferimento in modo generico alle verifiche effettuate ed alla documentazione acquisita, che verrà acquisita agli atti, senza fornire indicazioni, nell'atto, in merito ai certificati o documenti similari ottenuti. Salva diversa disposizione di legge, il titolare garantisce inoltre la riservatezza dei dati sensibili in sede di pubblicazione all'Albo on line o sul sito internet, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati. In ogni caso, inoltre, i documenti, soggetti a pubblicazione, riportanti informazioni di carattere sensibile o giudiziario dell'interessato, devono essere

anonimizzati con adeguate tecniche di anonimizzazione. I dati sensibili e giudiziari, infine, sono sottratti all'indicizzazione e alla rintracciabilità tramite i motori di ricerca web esterni ed il loro riutilizzo. Al momento non è prevista l'adozione di procedure organizzative per la cifratura dei dati personali.

La mappa completa delle misure di sicurezza procedurali, applicate ai diversi trattamenti è allegata al presente PPD per formane parte integrante e sostanziale, documenta e comprova l'osservanza del GDPR, con le stesse osservazioni effettuate ai punti precedenti.

Elenco delle misure di sicurezza

Fa parte integrante e sostanziale del sistema di protezione l'allegato elenco delle misure di sicurezza, correlate alla ricognizione/indice dei trattamenti e suddivise per uffici. Nell'allegato contenente gli acronimi delle misure di sicurezza programmabili è stata inserita la specifica indicazione sulle misure attuate "a.", non attuate/non previste ("n.a."), parzialmente attuate ("p.a."), da attuare a breve.

Registro delle attività di trattamento

A seguito delle attività di cui sopra si è proceduto, quando necessario, all'aggiornamento del Registro delle attività di trattamento. Nello specifico, fanno parte del sistema di protezione, anche se non materialmente allegati:

- il Registro delle attività di trattamento svolte sotto la responsabilità del titolare;
- il Registro delle attività di trattamento per ufficio.

I contenuti dei Registri devono essere conformi alle disposizioni contenute nell'articolo 30 del GDPR nonché alle prescrizioni della normativa interna di adeguamento del GDPR e alle linee guida, raccomandazioni, indicazioni e eventuali modelli del Garante.

Si precisa che, non svolgendo alcuna attività di Responsabile esterno del trattamento dei dati, l'EGAS non predispose alcun registro in tal senso.

Piano formativo

Il piano formativo deve essere impostato sulla base dei seguenti criteri:

a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali;

b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del GDPR;

c) Identificazione di procedure idonee per selezionare e formare i soggetti del sistema di protezione, come identificati nel presente PPD, da formare adeguatamente.

In prosecuzione del percorso formativo avviato in materia di privacy con l'affidamento del servizio di adeguamento agli obblighi previsti nel Regolamento europeo in materia di protezione dei dati personali (Regolamento UE 2016/679 o GDPR) e con l'acquisto del pacchetto All-Privacy, con circolare del 9 ottobre 2024, prot. n. 6164, era stata fornita apposita informativa ai dipendenti in merito ai corsi di formazione aggiornati disponibili nel sito www.entionline.it., con indicazioni di dettaglio sul programma completo disponibile nel software, sui corsi da seguire per ciascun dipendente in base alle funzioni svolte nell'Ente e sulle tempistiche da rispettare per l'assolvimento dell'obbligo formativo. Era stato anche reso disponibile un apposito modulo ai fini della dichiarazione di avvenuta frequentazione dei corsi, nonché un link per accedere ai quiz, da effettuare alla conclusione di ciascun corso per ottenere i relativi attestati.

Anche nel 2025 saranno fornite indicazioni di dettaglio sul programma dei corsi da seguire per ciascun dipendente. Si è in attesa, allo stato attuale, dell'aggiornamento del programma dei corsi disponibile nel software in dotazione dell'Ente.

Social network

L'utilizzo dei canali social è diventato molto frequente comune e di uso oramai ordinario anche da parte delle pubbliche amministrazioni al fine della diffusione di dati, informazioni e contenuti multimediali nonché della promozione dei servizi offerti.

Internet ed i social-network costituiscono, infatti, strumenti fondamentali:

- per l'esternazione della libertà di pensiero e di espressione, così come sancito dall'art. 21 della Costituzione e dall'art. 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali;
- per il rafforzamento della cittadinanza attiva e luogo di accesso semplice ed immediato alle informazioni;
- per la promozione delle notizie, dell'immagine e delle peculiarità dell'Ente e del territorio rappresentato.

L'utilizzo dei suddetti canali, laddove non regolamentato, può tuttavia dare luogo a illeciti trattamenti di dati personali.

A tale fine, acquisisce importanza strategica la circostanza che l'Ente si doti di un Regolamento per l'utilizzo dei social network, che disciplini la gestione ed il funzionamento dei profili istituzionali sui social network dell'Ente, garantendo l'espressione corretta delle informazioni.

A tal fine si rinvia al documento approvato con la Deliberazione del CIA n. 18 del 16 giugno 2022, di aggiornamento del PPD 2022/2024.

Si precisa, tuttavia, che con il DPR 13 giugno 2023, n. 81, sono state approvate alcune modifiche al DPR 16 aprile 2013, n. 62, recante "*Codice di comportamento dei dipendenti pubblici a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165*", riguardanti anche l'utilizzo dei mezzi di informazione e dei social media, che sono state recepite nel codice di comportamento dei dipendenti EGAS, aggiornato con la DCIA n. 44 del 14 dicembre 2023.

Posta elettronica e internet

Con provvedimento del 1 dicembre 2022 il Garante della Privacy ha sanzionato un ente pubblico per il monitoraggio posto in essere sulla posta elettronica del personale in servizio. Nel corso dell'istruttoria, l'Amministrazione aveva dichiarato di aver avviato una verifica interna sulla base del sospetto di una possibile rivelazione a terzi di informazioni protette dal segreto d'ufficio. Oggetto del monitoraggio, i metadati relativi ad orari, destinatari, oggetto delle comunicazioni, peso degli allegati.

Il Garante ha accertato che l'Ente aveva potuto effettuare il monitoraggio del personale sfruttando i dati conservati per generiche finalità di sicurezza informatica per 180 giorni (in luogo dei 7 consentiti dalla legge), in assenza di idonei presupposti giuridici, violando così i principi di protezione dei dati e delle norme sul controllo a distanza.

Il Garante ha così ribadito che la generalizzata raccolta e l'estesa conservazione dei metadati della posta elettronica - che in quanto forma di corrispondenza è tutelata dalla Costituzione - non sono strumentali allo "svolgimento della prestazione" del dipendente, ai sensi dello Statuto dei lavoratori.

Sulla base di ciò e dopo aver richiamato quanto indicato dal Garante della Privacy anche con le Linee guida per posta elettronica e internet del 5 marzo 2007, il DPO ha suggerito di predisporre un regolamento per l'utilizzo della posta elettronica e di internet al fine di rendere edotti i lavoratori in merito alle modalità di effettuazione degli eventuali controlli in relazione all'utilizzo degli strumenti informatici da parte dei dipendenti, nonché, più in generale, sull'utilizzo degli strumenti informatici.

Sulla base del modello predisposto dal DPO, l'EGAS ha così elaborato, ad integrazione della disciplina già dettata con il "Regolamento sulla protezione dei dati personali adottato in attuazione del Regolamento (UE) 2016/679" di cui alla Deliberazione del CIA n. 15 del 15 aprile 2020, apposito regolamento, approvato unitamente al Piano 2023/2025. Nella predisposizione dello stesso si è tenuto conto del sopracitato DPR 81/2023, le cui disposizioni hanno riguardato anche l'utilizzo delle tecnologie informatiche, recepite, così come detto per l'utilizzo dei mezzi di informazione e dei social media, nel codice di comportamento dei dipendenti EGAS.

Whistleblowing

Il 15 marzo 2023 è stato pubblicato il D.Lgs. 10 marzo 2023, n. 24, che dà attuazione in Italia alla Direttiva UE 2019/1937, tracciando le nuove regole di gestione delle segnalazioni di illeciti e rafforzando notevolmente la tutela dei segnalanti da possibili ritorsioni, prevedendo ex lege un'inversione dell'onere della prova.

Come previsto dall'art. 24 del Decreto, lo stesso è entrato in vigore a partire dal 15 luglio 2023.

Il Decreto disciplina la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato. Ogni trattamento di dati personali connesso alla ricezione e gestione delle segnalazioni dovrà dunque tener conto e conformarsi agli obblighi previsti dal GDPR.

Il D.Lgs 24/2023, all'art. 2 comma 1 lett. a n. 3, estende espressamente l'ambito di segnalazione "*a illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali indicati nell'allegato al presente decreto ovvero degli atti nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nell'allegato al presente decreto, relativi ai seguenti settori: protezione dei dati personali e sicurezza delle reti e dei sistemi informativi*".

La norma, quindi, prevede espressamente che sul canale di segnalazione whistleblowing possano essere segnalati al Responsabile della Prevenzione della corruzione anche trattamenti illeciti di dati.

Qualora la segnalazione riguardi un reclamo da parte del dipendente pubblico dell'Ente sul trattamento dei propri dati personali da parte del superiore gerarchico o dell'Ente Titolare del trattamento, chi gestisce la piattaforma, informando il DPO, deve, in applicazione della prescrizione posta dall'art. 13, comma 2 del D.lgs. 24/2023:

- cancellare immediatamente tutta la documentazione contenente dati personali manifestamente non utili ad un trattamento. Infatti, in tal caso, dare seguito alla segnalazione della violazione privacy riguardante lo stesso whistleblower potrebbe determinare l'avvio di un trattamento illecito, stante l'insussistenza di una finalità e di una adeguata base giuridica;
- dare, contestualmente, comunicazione al whistleblower, dell'avvenuta cancellazione, invitandolo a presentare rituale reclamo all'Autorità Garante della Privacy, indicando l'indirizzo del sito dell'Autorità

  https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/4535524#:~:text=L%27apposita%20istanza%20all%27Autorità,rpd%40gpdp.it)

Qualora, invece, la segnalazione riguardi il trattamento di dati personali da parte dell'Ente Titolare del Trattamento e che non riguardino ipotesi di reclamo, deve essere coinvolto il DPO perché assista l'Ente nell'adottare ogni iniziativa utile a verificare la fondatezza della segnalazione e ad attivare le azioni conseguenti per interrompere il trattamento illecito, nonché a valutare la sussistenza delle condizioni del data breach, da notificare al Garante della Privacy entro 72 ore dall'accertamento.

La nuova disciplina richiede poi che venga creato un "sistema" che consenta la segnalazione protetta e che il segnalante venga effettivamente protetto da ritorsioni conseguenti alla propria segnalazione.

Il D.lgs 24/2023 dispone, infatti, all'art. 4, che gli Enti realizzino *"*propri canali di segnalazione*, che garantiscano,* anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante*, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché' del contenuto della segnalazione e della relativa documentazione",* prevedendo le misure di sicurezza da adottare e i soggetti che devono gestire tale sistema*.*

L'eventuale soggetto esterno incaricato per la fornitura della piattaforma deve essere designato Responsabile del trattamento dei dati ai sensi dell'art. 28 del Regolamento UE 2016/679.

Il Responsabile della Prevenzione e della Corruzione che accede alla piattaforma deve essere autorizzato dal legale rappresentante dell'Ente a trattare tali dati con un atto specifico.

I dati poi devono essere conservati per un periodo di tempo congruo rispetto alle finalità perseguite, che può essere individuato in un termine di 18 mesi, salva diversa specifica valutazione.

Deve inoltre essere prevista una specifica informativa privacy ai sensi dell'art. 13 del GDPR, da consegnare al soggetto segnalante quando conferisce i propri dati per la segnalazione.

Da ultimo, si segnala che il D.Lgs 24/2023, all'art. 13, al comma 6, dispone che "*I soggetti di cui all'articolo 4 definiscono il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo n. 51 del 2018".*

Pertanto, prima di avviare l'utilizzo di una piattaforma whistleblowing è necessario redigere la valutazione di impatto da inviare al DPO per il parere di competenza.

Al riguardo si ricorda che con la Deliberazione del CIA n. 47 del 13 ottobre 2021 l'EGAS ha stabilito di:

- aderire al progetto "Whistleblowing PA" in linea con le misure generali previste nel piano anticorruzione, triennio 2021-2023, dando atto che – una volta attivata - il link alla piattaforma di segnalazione crittografata sarebbe stato rinvenibile nella Sezione Amministrazione Trasparente/Altri contenuti-Prevenzione della corruzione;
- aggiornare ed integrare in tal senso il documento recante "Procedura di segnalazione di illeciti o di irregolarità. Disciplina della tutela del dipendente pubblico che segnala illeciti (cd whistleblower)" (all. A), unitamente all'all.to 1 allo stesso "Modulo per la segnalazione di condotte illecite da parte del dipendente pubblico ai sensi dell'art. 54-bis del d.lgs. 165/2001".

I dati sono, dunque, raccolti tramite la piattaforma WhistleblowingPA, gestita da Whistleblowing Solutions S.r.l., che opera in qualità di Responsabile del trattamento designato dall'Ente ai sensi dell'art. 28 del Regolamento UE 2016/679, come risulta anche dall'informativa pubblicata nel sito dell'Ente. È stata inoltre redatta la relativa valutazione di impatto, inviata nell'anno 2022 al DPO, unitamente alle altre effettuate dall'Ente, per il parere di competenza.

L'Ente risultava, dunque, già in regola rispetto alle suddette prescrizioni. Il D.Lgs. 24/2023 è stato comunque analizzato nella sua interezza al fine di valutare eventuali aggiornamenti e modifiche da apportare al Regolamento dell'Ente e/o all'informativa di cui sopra. Ciò anche alla luce dell'approvazione della Deliberazione n. 311 del 12 luglio 2023, con cui l'ANAC ha adottato apposite linee guida, che hanno superato quelle approvate da ultimo con la Deliberazione n. 469 del 9 giugno 2021. Con la Deliberazione del CIA n. 51 del 28 dicembre 2023 è stato pertanto aggiornato ed integrato in tal senso il documento recante "Procedura di segnalazione di illeciti o di irregolarità. Disciplina della tutela del dipendente pubblico che segnala illeciti (cd whistleblower)" unitamente al "Modulo per la segnalazione di condotte illecite da parte del dipendente pubblico". Nel corso del 2024 il Documento è stato oggetto di monitoraggio, alla luce dell'iniziativa dell'ANAC, che ha approvato il documento "Linee guida whistleblowing sui canali interni di segnalazione - Consultazione on line - 07.11.2024". I risultati complessivi del monitoraggio sono riportati nel

documento allegato alla “Verifica dello stato di attuazione del Codice di comportamento dei dipendenti EGAS”.

ALLEGATI

1 Struttura organizzativa e soggetti:

- 1.a struttura organizzativa
- 1.b elenco soggetti interni
- 1.c responsabili esterni
- 1.d sub responsabili esterni
- 1.e titolari autonomi
- 1.f altri soggetti

2 schede di ricognizione e elenco trattamenti:

- 2.a assoggettabilità
- 2.b elenco dei trattamenti

3 DPIA

4 Mappa dei luoghi:

- 4.a sede istituzionale
- 4.b elenco uffici

5 Hardware software archivi e banche dati elettroniche:

- 5.a caratteristiche tecniche strumenti elettronici
- 5.b. elenco archivi e banche dati
- 5.c server
- 5.d strumenti

6 Mappa rischi e motivazioni di stima – eventi rischiosi stimati

7 Misure di sicurezza:

- 7.a. misure di sicurezza protezione dati
- 7.b. misure-informatiche e rischi contrastati
- 7.c. misure logistiche e rischi contrastati
- 7.d. misure-organizzative e rischi contrastati
- 7.e. misure-procedurali e rischi contrastati
- 7.f. acronimi-misure e stato di attuazione

8 Corsi di formazione