SSM

Scuola Superiore Meridionale

PROCEDURA

PER LA GESTIONE DELLA PROTEZIONE DEI DATI PERSONALI

INDICE

1. GENERALITÀ

1.1 SCOPO

La presente procedura definisce le regole generali adottate dalla **Scuola Superiore Meridionale** per la disciplina degliadempimenti connessi al Trattamento dei Dati Personali.

In particolare, la procedura ha l'obiettivo di:

- stabilire ruoli e responsabilità dei principali soggetti coinvolti nel Trattamento dei Dati Personali;
- definire le modalità operative più idonee a garantire il rispetto delle previsioni normative con specifico riferimento alle figure chiave previste, ai termini e alle condizioni per l'acquisizione e la gestione dei Dati Personali, ai diritti degli Interessati nonché all'eventuale gestione dei rapporti con l'Autorità Garante;
- definire ruoli, responsabilità, modalità operative e regole da seguire per la gestione e la soluzione di eventuali criticità concernenti i Dati Personali posseduti o trattati;
- fornire la modulistica e gli atti standard da utilizzare obbligatoriamente per la gestione degli adempimenti suddetti.

1.2 CAMPO D'APPLICAZIONE

La presente procedura si applica a tutti i settori del Titolare del Trattamento.

Si precisa che la presente procedura (unitamente a tutte le definizioni fornite ed applicabili nel presente documento) è riferita al Titolare del Trattamento ed ai Trattamenti di Dati Personali, non solo propri ma anche di terzi, dallo stesso effettuati.

In ogni caso, rientrano nella presente procedura eventuali operazioni di Trattamento dei Dati Personali di titolarità/responsabilità di terzi, qualora il Titolare del Trattamento o propri esponenti sia/siano nominati soggetti autorizzati al trattamento e qualora soggetti esterni siano nominati Responsabili del Trattamento. Rientrano altresì nella presente procedura i Trattamenti per i quali il Titolare del Trattamento nomini terzi Responsabili e/o Autorizzati: in tali casi, i terzi dovranno attenersi alle regole e prescrizioni ivi previste.

Rimane fermo l'obbligo di valutare, ai sensi della presente procedura, se sia obbligatorio per il Titolare del Trattamento nominare/essere nominati Responsabili/Autorizzati in relazione ai trattamenti di Dati Personali da effettuarsi nel corso delle proprie attività.

1.3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 196/2003 e s.m.i. (Codice in materia di protezione dei Dati Personali – "**Codice Privacy**");

- Regolamento UE 2016/679 in materia di protezione dei Dati Personali e della relativa circolazione ("**Regolamento**");
- Art.29 Working party Doc.248: "Guidelines on Data Protection Impact Assessment" – (rev. del 4.10.2017);
- Art. 29 Working party Doc. 243: "Linee guida sui responsabili della protezione dei dati personali";
- Art. 29 Working party Doc. 242: "Linee guida sul diritto alla portabilità dei dati".

1.4 PRINCIPI GENERALI

Le funzioni interne coinvolte nelle attività di raccolta, conservazione ed utilizzo di Dati Personali operano nel rispetto del sistema normativo interno e del sistema di poteri e responsabilità, nonché in piena conformità con tutte le leggi ed i regolamenti vigenti, ispirandosi ai seguenti principi fondamentali:

- ogni Trattamento dei Dati Personali deve svolgersi nel **rispetto dei diritti e delle libertà fondamentali e della dignità dell'Interessato**, con particolare riferimento alla riservatezza, all'identità personale ed al diritto alla protezione dei Dati Personali, in coerenza con i principi normativi previsti per il loro esercizio;
- ogni Trattamento è ammesso purché i Dati Personali:
  i. siano trattati **in modo lecito**, **corretto** e **trasparente** nei confronti dell'Interessato;
  ii. siano raccolti per **finalità determinate**, **esplicite** e **legittime** e successivamente trattati in un modo che sia compatibile con tali finalità;
  iii. siano **adeguati**, **pertinenti** e **limitati** a quanto necessario rispetto alle finalità per le quali sono trattati;
  iv. siano **esatti** e, se necessario, **aggiornati**;
  v. siano adottate tutte le misure ragionevoli per **cancellare o rettificare** tempestivamente i Dati inesatti ovvero irrilevanti rispetto alle finalità per le quali sono trattati;
  vi. siano **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;
  vii. siano trattati in maniera da garantirne un'adeguata sicurezza, compresa la protezione mediante **misure tecniche e organizzative adeguate**;
- laddove necessario, il Titolare del Trattamento attraverso le figure chiave previste dal Regolamento, **collabora con l'Autorità Garante**, anche con riferimento specifico ad eventuali casi di notifica per violazioni ovvero in relazione alla valutazione preliminare per il Trattamento di taluni Dati, allo scopo di garantire il pieno rispetto dei diritti dell'Interessato e di fornire tutte le informazioni necessarie all'Autorità Garante;
- ogni Trattamento dei Dati Personali deve essere avviato in maniera trasparente, rendendo all'Interessato idonea **Informativa** in merito alle finalità, tempistiche, comunicazione e diffusione del Trattamento stesso e acquisendone, in tutti i casi previsti dalla legge, il **Consenso** in maniera formale, scritta e libera;
- ogni Trattamento dei Dati Personali sarà avviato ed effettuato nel rispetto del principio di "**Minimizzazione e riduzione**" e **Privacy By Design**", previsti dal Regolamento: pertanto, il Trattamento dei dati sarà improntato a trattare e conservare i soli dati strettamente necessari

per lo svolgimento delle specifiche attività interne, nonché alla riduzione al minimo e alla pseudonimizzazione, ove possibile, dei Dati Personali trattati e conservati.

2. TERMINI E DEFINIZIONI

Termine	Definizione
DATO PERSONALE	Qualunque informazione relativa a persona fisica (es.: nome, cognome, codice fiscale, data di nascita), identificata o identificabile, **direttamente mediante il dato o anche indirettamente**, mediante riferimento a qualsiasi altra informazione, ivi compreso il numero di identificazione personale (es.: codice identificativo dipendente, associazione nome e cognome e numero di telefono mobile) o anche a 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.
DATO PARTICOLARE	Dato Personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche e di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché il Dato Personale idoneo a rivelare lo stato di salute e la vita sessuale.
DATO RELATIVO A CONDANNE PENALI E REATI	Dato Personale idoneo a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 (Assunzione della qualità di imputato) e 61 (Estensione dei diritti e delle garanzie dell'imputato) del codice di procedura penale, nonché le misure di sicurezza connesse ai reati.
AUTORITÀ GARANTE	L'Autorità denominata Garante per la protezione dei dati personali di cui all'articolo 153 del Codice Privacy, che, tra l'altro, controlla se i Trattamenti siano effettuati nel rispetto della disciplina di legge applicabile. Per l'Italia, tale Autorità è il Garante per la Protezione dei Dati Personali.
INTERESSATO	Una persona fisica, identificata o identificabile mediante Dati Personali, titolare dei relativi Diritti dell'Interessato, come definiti e dettagliati nella presente procedura.
TRATTAMENTO DEI DATI PERSONALI **("TRATTAMENTO")**	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a Dati Personali o insiemi di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, 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.
TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI **("TITOLARE")**	Il soggetto che assume le decisioni in ordine alle finalità e alle modalità del Trattamento dei Dati Personali nonché agli strumenti utilizzati, ivi compresi gli atti di nomina delle figure interne preposte e il sistema di regole e procedure da seguire. Il Titolare è identificato nella persona del suo legale rappresentante *pro tempore*. Il termine "Titolare", laddove la regola prevista nella procedura è di generale applicazione, va inteso come riferimento a qualsiasi Titolare, anche terzo.

RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI **("RESPONSABILE")**	Il soggetto (persona fisica o giuridica) esterno cui il Titolare affida con specifico atto di nomina, per la particolare esperienza o capacità, compiti di gestione e controllo del Trattamento dei Dati Personali, unitamente alle relative responsabilità. Ai sensi del Regolamento, il Responsabile può essere individuato *esclusivamente* tra persone e/o società terze, rispetto all'organizzazione del Titolare, e pertanto non è più possibile, come in vigenza del solo Codice Privacy, nominare Responsabili persone fisiche interne. Il Responsabile può nominare Autorizzati al Trattamento, per lo svolgimento delle specifiche attività e Trattamenti a lui assegnati dal Titolare.
AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI **("AUTORIZZATO")**	La persona fisica che, con formale atto di nomina *ad personam* ovvero per unità organizzativa, elabora o utilizza materialmente i Dati Personali sulla base delle istruzioni ricevute dal Titolare che lo nomina. L'Autorizzato può essere un dipendente o comunque un soggetto interno all'Ente. L'Autorizzato è nominato ai sensi dell'art. 2-quaterdecies del D. Lgs. n. 196/2003.
AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI CON FUNZIONI DI REFERENTE **("AUTORIZZATO REFERENTE" o "REFERENTE")**	La persona fisica, interna al Titolare del Trattamento, che, con formale atto di nomina *ad personam*, elabora o utilizza materialmente i Dati Personali sulla base delle istruzioni ricevute dal Titolare del Trattamento che lo nomina, agendo al tempo stesso quale referente e soggetto deputato alla gestione ed organizzazione degli Autorizzati nello specifico reparto di competenza, interno al Titolare. L'Autorizzato è nominato ai sensi dell'art. 2-quaterdecies del D. Lgs. n. 196/2003.
RESPONSABILE DELLA PROTEZIONE DEI DATI **(anche "Data Protection Officer - DPO")**	Il soggetto a cui, con atto di nomina a firma del Titolare/Responsabile del Trattamento, in funzione delle qualità professionali - in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei Dati Personali, con il supporto di adeguate risorse organizzative e di budget -, sono assegnati i compiti di fornire supporto e consulenza al Titolare ed agli Autorizzati, di vigilare sull'applicazione delle normative e delle procedure, di fornire assistenza agli Interessati e di collaborare con l'Autorità Garante e/o con le altre Autorità, fungendo quale punto di contatto unico.
AMMINISTRATORE DI SISTEMA	Il soggetto che ai sensi della presente procedura e sulla base delle indicazioni di volta in volta impartire dal Titolare, dai Responsabili e dal DPO, si occupa della gestione e della manutenzione di un impianto di elaborazione o di sue componenti; in tale categoria, rientrano altresì le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi. L'amministratore di sistema è un ruolo operativo, essenziale per la sicurezza dei sistemi informatici e telematici e delle banche dati, dotato quindi di specifiche competenze tecniche, al quale è affidato il compito della gestione di tali sistemi, autorizzando altri soggetti (sempre in base alle istruzioni ricevute) all'accesso ai sistemi (ad es. registrazione degli accessi logici degli autorizzati, accessi logici separati, ecc...), oltre al compito di vigilare sull'utilizzo dei sistemi. Nel suo ruolo, l'amministratore di sistema è il soggetto principale con riferimento alle problematiche dei data breach. Nel caso in cui tale ruolo sia esternalizzato, l'amministratore di sistema sarà un responsabile del trattamento.
MISURE DI SICUREZZA	Il complesso delle misure tecniche e organizzative, comprese le misure informatiche, adottate per ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei Dati Personali, di accesso non autorizzato o di Trattamento non consentito o non conforme alle finalità della raccolta.

INFORMATIVA	L'atto (nella prassi denominato anche "Privacy policy"), con il quale il Titolare si identifica rendendo note agli Interessati le previsioni normative nonché le modalità di raccolta e archiviazione dei Dati Personali, le finalità e le modalità di Trattamento degli stessi, nonché il riferimento al DPO. Si tratta di un documento comunicato agli Interessati preliminarmente all'avvio di un Trattamento, che può essere loro consegnato in copia oppure reso ad essi disponibile con altre modalità adeguate ad assicurare di conoscenza di dette previsioni, finalità e modalità.
CONSENSO DELL'INTERESSATO	La manifestazione di volontà libera, specifica, informata e inequivocabile (di regola per iscritto) dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante la dichiarazione prevista ai sensi della presente procedura, al Trattamento dei Dati Personali che lo riguardano. Il consenso viene raccolto secondo le modalità previste nella presente procedura, nel rispetto delle previsioni di legge e delle indicazioni dell'Autorità Garante, che individuano in maniera precisa i singoli Trattamenti per i quali viene richiesto il consenso dell'Interessato, che deve essere, ove prescritto, richiesto e reso in relazione a specifici Trattamenti descritti nell'Informativa.
DIRITTI DELL'INTERESSATO	I diritti che l'Interessato può esercitare presso i soggetti che trattano i suoi Dati Personali o che egli presume trattino Dati Personali che lo riguardino, ai sensi del Regolamento e del Codice Privacy e delle specifiche disposizioni della presente procedura.
VIOLAZIONE **(anche "DATA BREACH")**	Qualsiasi violazione e/o anomalia inerente al Trattamento di Dati Personali, che comporti l'insorgere e/o l'aggravarsi dei rischi per gli Interessati. A titolo d'esempio non esaustivo, un Data Breach può essere costituito dalla distruzione accidentale o perdita dei Dati Personali, dalla loro divulgazione e/o diffusione a qualsiasi titolo presso soggetti e/o autorità non autorizzati, la loro indebita modificazione, copia o rimozione in assenza delle necessarie autorizzazioni, del consenso dell'Interessato e/o comunque in violazione di norme di legge o prescrizioni dell'Autorità Garante. Il Data Breach dovrà essere notificato dal Titolare del Trattamento, in accordo con il DPO, all'Autorità Garante nonché comunicato all'Interessato, secondo le modalità e nei casi previsti dalla presente procedura in conformità al Regolamento.
VALUTAZIONE D'IMPATTO **(anche "Data Protection Impact Assessment – "DPIA")**	L'analisi (di regola preventiva) relativa all'avvio, alla prosecuzione o alla modifica delle operazioni di Trattamento di una o più tipologie di Dati Personali, che per la loro delicatezza, particolarità, diffusività o invasività (in particolare qualora vi sia l'uso di nuove tecnologie) possono comportare rischi elevati per l'Interessato. Detta analisi, che deve essere compiuta dai competenti Responsabili del Trattamento secondo le regole stabilite nella presente procedura (anche con riguardo ai profili oggetto di valutazione e alla loro rendicontazione), è volta ad individuare i principali problemi nelle operazioni di Trattamento e a predisporre strumenti per la loro soluzione.
REGISTRO DEI TRATTAMENTI	Il registro, istituito e conservato dal DPO per conto del Titolare ed alimentato da ciascun Responsabile del Trattamento, in cui sono censite ed individuate le attività di Trattamento di Dati Personali svolte dal Titolare del Trattamento, secondo le regole stabilite dalla presente procedura in linea con le disposizioni del Regolamento.

RUOLI E RESPONSABILITÀ

Attività:	Tit	Res	Aut	Aut.Ref	DPO	Amm	Int	AG
Titolare del Trattamento dei Dati Personali								
Definire le finalità e le modalità dei Trattamenti dei Dati Personali	*	+						
Nominare e revocare i Responsabili dei Trattamenti e il DPO	*							
Nominare e revocare Autorizzati dei Trattamenti	*							
Nominare e revocare Amministratori di Sistema	*							
Nominare e revocare Autorizzati Referenti	*							
Sorvegliare circa il rispetto della normativa applicabile	*				+			
Responsabile del Trattamento dei Dati Personali								
Assistere il Titolare nell'adozione delle misure in materia di protezione dei Dati	+	*						
Garantire il rispetto della normativa applicabile in materia		*			+			
Svolgere il Data Protection Impact Assessment		*			+			
Individuare l'ambito di trattamento dei dati consentito agli Autorizzati		*						
Predisporre e fornire l'informativa agli interessati		*					**o**	
Fornire la documentazione di supporto al Titolare o al DPO	+	*			+			
Identificare l'Autorizzato al Trattamento dei Dati Personali		*						
Raccogliere, utilizzare, mantenere aggiornati e conservare i Dati Personali		*	*					
Trasmettere l'informativa periodica, con frequenza semestrale, al DPO		*			**o**			
Informare il DPO in caso di violazione dei Dati Personali (Data Breach Notification)		*			**o**			
Autorizzato Referente al Trattamento dei Dati Personali								
Coordinare l'azione degli Autorizzati di riferimento nella rispettiva area di competenza	+	+		*				
Compiere operazioni di trattamento dati (raccolta, registrazione, organizzazione…)			*					
Garantire il rispetto delle disposizioni normative dettate in materia		+	*		+			
Applicare tutte le misure di sicurezza con riferimento ai Trattamenti effettuati			*					
Partecipare ai corsi formativi in materia di privacy			*					
Comunicare qualunque notizia rilevante con riferimento al Trattamento dei Dati		**o**	*		**o**			
Fornire qualsiasi informazione necessaria per rispondere ad eventuali richieste	+	+	*		+			
Autorizzato al Trattamento dei Dati Personali								
Compiere operazioni di trattamento dati (raccolta, registrazione, organizzazione…)			*					
Garantire il rispetto delle disposizioni normative dettate in materia		+	*		+			
Applicare tutte le misure di sicurezza con riferimento ai Trattamenti effettuati			*					
Partecipare ai corsi formativi in materia di privacy			*					
Comunicare qualunque notizia rilevante con riferimento al Trattamento dei Dati		**o**	*		**o**			

Fornire qualsiasi informazione necessaria per rispondere ad eventuali richieste	+	+	*		+			
Responsabile della Protezione dei Dati (DPO)								

Attività:	Tit	Res	Aut	Aut.Ref	DPO	Amm	Int	AG
Sorvegliare l'osservanza del Codice Privacy e del Regolamento					*			
Monitorare l'evoluzione normativa in ambito privacy e provvedere all'aggiornamento del Titolare	o	o			*			
Aggiornare la presente procedura e supervisionare la sua applicazione					*			
Fornire consulenza al Titolare, agliAutorizzati e agli Interessati su materie inerenti il Trattamento dei Dati Personali	o	o	o		*		o	
Sovrintendere alla specifica sezione della intranet in materia di Privacy					*			
Promuovere l'organizzazione di attività di comunicazione e formazione in materia di Privacy					*			
Interagire e cooperare con l'Autorità Garante e con qualsiasi Autorità competente, nell'ambito delle indagini da queste compiute					*			+
Rispondere ad eventuali richieste, diffide e/o contestazioni di illecito/incorretto Trattamento a qualsiasi titolo inoltrate.					*			
Predisporre il Piano di Attività		+			*			
Predisporre un programma di verifiche sull'adeguatezza e sull'osservanza delle disposizioni in materia di privacy					*			
Richiedere documentazione o svolgere interviste afferenti i Trattamenti dei Dati Personali					*			
Chiedere informazioni in merito a segnalazioni ricevute da parte di Autorizzati/Interessati circa la violazione dei Dati Personali		o	o		*		o	
Predisporre la documentazione relativa alle attività condotte e concordare le necessarie azioni correttive		+	+		*			
Istituire e conservare il Registro dei Trattamenti		+			*			
Verificare la rilevanza e l'attendibilità dei fatti riferiti	o	o			*			
Riferire alla Direzione Gruppo Risorse Umane e Organizzazione sulla violazione delle disposizioni normative o procedurali					*			
Predisporre e trasmettere al Titolare una relazione semestrale di resoconto sulle attività svolte nel periodo di riferimento	o				*			
Notificare la violazione dei Dati Personali all'Autorità Garante in presenza di un rischio per i diritti e le libertà dell'Interessato					*			o
Amministratore di Sistema								
Adottare e gestire, con il supporto degli strumenti adeguati, le misure di sicurezza per la Protezione di Dati		+	+		+	*		
Identificare pratiche operative per la corretta gestione degli strumenti informativi						*		
Predisporre, revisionare, controllare e aggiornare le misure di sicurezza informatiche implementate		+			+	*		
Interessato								
Fornire, di regola in forma scritta, il consenso al Trattamento dei Dati Personali							*	

Esercitare i seguenti diritti: diritto di accesso, diritto di rettifica, diritto alla portabilità, diritto di limitazione al Trattamento, diritto di opposizione ad un Trattamento, diritto alla cancellazione (diritto all'oblio)							*	
Trasmettere l'informativa specifica al DPO					o		*	

Legenda: (*): Responsabilità primaria; (+): Collabora; (°): Deve essere informato

Tit: Titolare del Trattamento dei Dati Personali
Res: Responsabile del Trattamento dei dati Personali
Aut: Autorizzato al Trattamento dei Dati Personali
Aut.Ref: Autorizzato Referente al Trattamento dei Dati Personali
DPO: Responsabile della Protezione dei Dati Personali
Amm: Amministratore di Sistema
Int: Interessato
AG: Autorità Garante

3. MODALITÀ OPERATIVE

3.1 PRINCIPALI RUOLI IN MATERIA DI PRIVACY

4.1.1 Titolare del Trattamento dei Dati Personali

Ai fini della presente procedura, al Titolare del Trattamento dei Dati Personali competono le decisioni in ordine ai seguenti principali profili:

- definizione delle finalità e delle modalità dei Trattamenti di Dati Personali, nonché predisposizione delle misure tecniche e organizzative adeguate a garantire che ciascun Trattamento sia effettuato conformemente al Codice Privacy e al Regolamento, ivi compreso il profilo della sicurezza, anche avvalendosi delle analisi e delle valutazioni svolte dalle competenti funzioni interne;
- nomina e revoca dei Responsabili dei Trattamenti, degli Autorizzati, dei Referenti Interni e del DPO per la corretta gestione dei Trattamenti interni e degli adempimenti normativi;
- sorveglianza circa il rispetto della normativa in materia, anche avvalendosi del supporto del Responsabile della Protezione dei Dati Personali.

4.1.2 Il Responsabile del Trattamento dei Dati Personali ed il Referente

Il Responsabile del Trattamento (individuato in un soggetto terzo all'esterno della stessa) è designato nella figura che ricopre una posizione idonea per competenza tecnico/normativa (conoscenza delle disposizioni normative e procedurali applicabili e/o delle misure di sicurezza, nonché responsabilità di gestione o custodia delle banche dati o archivi dell'area), in maniera tale da consentirgli di mettere in atto misure tecniche e organizzative adeguate affinché il Trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'Interessato.

Il Responsabile del Trattamento dei Dati Personali è identificato attraverso un atto di nomina firmato

dal Titolare e sottoscritto dal Responsabile stesso per accettazione.

Le responsabilità attribuite a dette figure relativamente all'area di competenza sono, a titolo esemplificativo e non esaustivo, le seguenti:

- assistere il Titolare nell'adozione di tutte le misure in materia di protezione dei Dati Personali con riguardo alla propria area di competenza;
- nell'ambito delle attribuzioni conferitigli e con specifico riferimento ai Dati, prendere in piena autonomia le decisioni idonee a garantire il rispetto della vigente normativa in materia di protezione dei Dati Personali e adottare le misure e le particolari precauzioni necessarie ad un corretto trattamento dei Dati Particolari e Relativi a condanne penali e reati trattati dal Titolare;
- coordinarsi con il Responsabile della Protezione dei Dati al fine garantire il pieno rispetto delle disposizioni dettate dalla normativa applicabile in materia, coinvolgendolo non appena possibile sulle questioni riguardanti la protezione dei Dati;
- svolgere il Data Protection Impact Assessment relativamente ai Dati trattati nell'area di propria competenza, qualora ciò sia richiesto ai sensi della presente procedura, coordinandosi con il Responsabile della Protezione dei Dati sia in merito alla necessità di svolgere o meno detto Assessment sia con riguardo alla metodologia di svolgimento;
- effettuare le operazioni di Trattamento dei Dati, individuando, di volta in volta, le modalità da seguire affinché la raccolta, il trattamento e la conservazione degli stessi avvengano nel rispetto della normativa dettata dal Codice Privacy e dal Regolamento e dalla presente procedura;
- astenersi dall'adottare autonome decisioni in contrasto con le finalità e le modalità del Trattamento prescritte dal Titolare o dalla presente procedura e comunque non svolgere, di propria iniziativa, alcuna operazione di Trattamento - compresa la comunicazione e la diffusione a soggetti terzi - diversa da quelle indicate nell'Informativa consegnata agli Interessati e per cui sia stato rilasciato il Consenso;
- individuare l'ambito di Trattamento dei Dati Personali consentito agli Autorizzati (o, ove del caso, a soggetti esterni) al fine di permettere il corretto svolgimento delle attività istituzionalmente demandate alle aree in questione, fornendo a questi le necessarie istruzioni per un corretto adempimento delle norme del Codice Privacy, del Regolamento e della presente procedura ed altresì vigilando sul loro operato;
- controllare periodicamente l'efficacia delle misure di sicurezza adottate e la loro conformità alle disposizioni del Codice Privacy e del Regolamento e della presente procedura;
- adottare le misure idonee a consentire agli Interessati l'effettivo esercizio dei propri diritti, in particolare, agevolare senza ritardi l'accesso ai Dati da parte degli stessi, semplificando, ove possibile, le modalità per il riscontro delle relative richieste.

Inoltre, il Responsabile del Trattamento e l'Autorizzato Referente devono collaborare con il Titolare e/o con il Responsabile della Protezione dei Dati nell'esecuzione di ogni attività di verifica sull'adeguatezza e sull'osservanza della presente procedura. A tal fine, essi, su richiesta del Titolare e/o del Responsabile della Protezione dei Dati, sono tenuti a fornire la documentazione di supporto e comunicare a questi ultimi ogni informazione necessaria.

Gli eventuali soggetti terzi che svolgano per il Titolare del Trattamento attività in outsourcing che comportino l'eventuale Trattamento di Dati Personali, dovranno essere nominati al momento della stipula dell'ordine / contratto in qualità di Responsabile del Trattamento dei Dati Personali.

Inoltre, gli ordini / contratti con detti soggetti terzi devono prevedere apposite clausole contrattuali tramite le quali viene assicurata l'implementazione dei seguenti aspetti:

- la definizione della materia disciplinata;
- l'indicazione della durata del Trattamento;
- la natura e la finalità del Trattamento;
- la tipologia di Dati Personali trattati;
- le categorie di Interessati;
- gli obblighi e i diritti del Titolare;
- l'impegno alla riservatezza dei soggetti autorizzati al Trattamento dei Dati;
- l'adozione delle misure di sicurezza adeguate (compresi i vincoli di riservatezza);
- il rispetto degli obblighi di conservazione dei Dati Personali secondo le modalità previste dalla legge applicabile e nel rispetto delle indicazioni fornite dal Titolare in proposito;
- la messa a disposizione del Titolare di tutte le informazioni necessarie per dimostrare il rispetto degli obblighi assunti, impegnandosi a collaborare per attività di controllo;
- la messa a disposizione del Titolare del Trattamento, dell'Autorità Garante e delle altre Autorità competenti di tutte le informazioni necessarie per rispondere ad eventuali contestazioni e/o segnalazioni di illecito che dovessero essere inoltrate;
- la cancellazione o la restituzione al Titolare del Trattamento di tutti i Dati Personali al termine della prestazione di servizi relativi al Trattamento.

Il Responsabile del Trattamento è direttamente responsabile, sia nei confronti del Titolare che degli Interessati, per tutte le violazioni delle istruzioni e modalità operative fornitegli dal Titolare e per le operazioni di Trattamento che è chiamato a gestire ai sensi della presente procedura e dell'atto di nomina.

Si precisa altresì che il Responsabile del Trattamento assume sempre piena responsabilità per le operazioni di Trattamento compiute secondo le indicazioni del Titolare (comprese quelle previste nella presente procedura e nell'atto di nomina) e, con detto Titolare, è chiamato a rispondere di ogni violazione e Trattamento illecito/irregolare a cui dia anche involontariamente causa.

La responsabilità del Referente è invece "limitata", ed opera nei confronti del solo Titolare: qualora il Referente violi le istruzioni e le modalità operative fornitegli dal Titolare per le operazioni di Trattamento, sarà chiamato a risponderne a livello contrattuale solamente nei confronti di tale ultimo soggetto.

4.1.3 Autorizzato (persona Autorizzata) al Trattamento dei Dati Personali

L'Autorizzato al Trattamento dei Dati Personali è identificato da ciascun Titolare e/o Responsabile nell'ambito della propria area di competenza e deve attenersi strettamente alle istruzioni dallo stesso impartite in relazione alle specifiche finalità e modalità di utilizzo dei Dati Personali a cui lo stesso

abbia accesso.

L'Autorizzato effettua operativamente le attività di Trattamento dei Dati Personali attinenti all'attività lavorativa di competenza della sua area di appartenenza.

Il Titolare e/o il Responsabile, in funzione delle caratteristiche del Trattamento richiesto e della numerosità dei Dati trattati, potrà identificare uno o più Autorizzati.

Le responsabilità attribuite a detta figura relativamente all'area di competenza sono, a titolo esemplificativo e non esaustivo, le seguenti:

- compiere le operazioni di trattamento, ovvero di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione, distribuzione dei Dati, unicamente per gli scopi strettamente inerenti l'attività svolta. In particolare, le operazioni di trattamento eseguite devono essere pertinenti e non eccedenti le finalità per le quali i Dati sono stati raccolti, verificandone l'esattezza e, se necessario, procedendo alla correzione e all'aggiornamento;
- coordinarsi con il Responsabile del Trattamento e/o con il Referente, anche per l'ulteriore coordinamento di questi con il DPO, al fine garantire il pieno rispetto delle disposizioni dettate dalla normativa applicabile in materia (compresi i contenuti dell'Informativa e del Consenso);
- rispettare il divieto di comunicazione e diffusione dei Dati trattati contenuti nelle banche dati: in particolare, la comunicazione/diffusione dei Dati potrà avvenire solo previa specifica autorizzazione del Titolare;
- applicare tutte le misure di sicurezza con riferimento ai Trattamenti effettuati, sia con strumenti elettronici (compreso l'utilizzo delle credenziali di autenticazione) che senza (compresa l'idonea custodia e conservazione di atti e documenti), segnalando al Responsabile ed al Referente eventuali rischi di distruzione o perdita, anche accidentale, dei Dati, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta;
- partecipare ai corsi formativi organizzati dal Responsabile della Protezione dei Dati e/o dal Referente in materia di Privacy e alle altre iniziative di divulgazione;
- comunicare al Responsabile, al Referente e al DPO qualunque notizia reputi rilevante con riferimento al trattamento dei dati personali compresa qualsiasi circostanza in cui vi sia violazione ovvero incertezza nell'interpretazione e nell'applicazione delle regole;
- collaborare con il Titolare, il Responsabile, il Referente ed il DPO al fine di fornire qualsiasi informazione necessaria per rispondere ad eventuali richieste, diffide e/o contestazioni di illecito/incorretto Trattamento che siano trasmesse dall'Autorità Garante e/o delle altre Autorità competenti.

4.1.4 Responsabile della Protezione dei Dati (DPO)

Il Responsabile della Protezione dei Dati opera a supporto del Titolare e dei Responsabili/Referenti fornendo assistenza e consulenza su tutte le tematiche concernenti la protezione dei Dati Personali.

Il DPO ha il compito generale di sorvegliare l'osservanza del Codice Privacy e del Regolamento, ferma restando la responsabilità del Titolare e dei Responsabili del Trattamento in caso di mancato rispetto delle suddette disposizioni normative.

In particolare, al Responsabile della Protezione dei Dati sono attribuiti i seguenti compiti principali:

- monitorare l'evoluzione normativa in ambito Privacy, le decisioni e le interpretazioni dell'Autorità Garante e della giurisprudenza, nonché provvedere all'aggiornamento del Titolare e dei Responsabili in merito agli eventuali impatti sul Titolare stesso;
- supervisionare l'applicazione della presente procedura e della relativa modulistica curandone gli aggiornamenti che dovessero rendersi necessari;
- fornire consulenza al Titolare, al Responsabile, agli Autorizzati Referenti, agli Autorizzati e agli Interessati su materie inerenti al Trattamento dei Dati Personali, con particolare riferimento: alla valutazione dei rischi connessi ai Trattamenti (Data Protection Impact Assessment) e alla redazione/aggiornamento di tutta la documentazione rilevante in materia di protezione dei dati personali (es. registro dei trattamenti, informative, consensi, clausole contrattuali, atti di nomina, ecc.);
- sovrintendere alla specifica sezione della intranet contenente tutta la documentazione in materia di protezione dei dati personali;
- promuovere l'organizzazione di attività di comunicazione e formazione in materia di protezione dei dati personali;
- interagire e cooperare con l'Autorità Garante operando con questa da punto di contatto, con riguardo, tra l'altro, alla consultazione preventiva a seguito di un Data Protection Impact Assessment, alle segnalazioni di possibili violazioni ed alla gestione e facilitazione di eventuali ispezioni;
- interagire e cooperare con qualsiasi Autorità competente, nell'ambito delle indagini da queste compiute, nonché ove sia necessario rispondere ad eventuali richieste, diffide e/o contestazioni di illecito/incorretto Trattamento a qualsiasi titolo inoltrate.

4.1.5 Amministratore di Sistema

L'Amministratore di Sistema è la figura professionale che, in ambito informatico, mantiene, configura e gestisce, in quanto amministratore di sistema, anche con riguardo ai profili Privacy: (i) i sistemi di elaborazione dei Dati o sue componenti, ivi inclusi i sistemi software; (ii) una base dati; e (iii) reti e apparati di telecomunicazione.

L'Amministratore di Sistema supporta il Titolare, i Responsabili del Trattamento dei Dati Personali, i Referenti Interni nonché il DPO per lo svolgimento dei loro rispettivi compiti, qualora questi comportino l'utilizzo di strumenti informatici, in particolare mediante:

- l'individuazione, l'adozione e l'implementazione delle misure di sicurezza informatiche idonee ad assicurare la protezione di Dati (misure per la prevenzione da intrusioni e perdite degli stessi);
- la definizione degli strumenti adeguati ad assicurare l'effettivo esercizio dei diritti degli Interessati (es. accesso, cancellazione, portabilità);
- l'identificazione delle pratiche operative per la corretta gestione degli strumenti informativi (es. utilizzo delle dotazioni informatiche) nonché per attivare le necessarie azioni in caso di perdita dei dati o di problematiche inerenti alla riservatezza ed alla sicurezza informatica;
- la revisione ed il controllo delle misure di sicurezza informatiche implementate, anche

inoccasione dello svolgimento di un'Analisi di Impatto.

3.2 MODALITÀ DI GESTIONE DEI DATI

3.2.1 Registro dei Trattamenti

Il Titolare è tenuto a redigere e conservare un Registro dei Trattamenti. Detto Registro è tenuto all'interno di un'apposita sezione della Intranet a cui hanno accesso, oltre al Responsabile della Protezione dei Dati, anche i Responsabili del Trattamento, i Referenti Interni e gli Autorizzati, nonché il Titolare.

Ciascun Autorizzato e/o Referente alimenta il Registro inserendo tutte le informazioni attinenti i propri Trattamenti e ne cura il relativo aggiornamento. In particolare, l'Autorizzato / il Referente inserisce all'interno del Registro tutte le informazioni connesse:

- ai Trattamenti effettuati;
- all'avvio di un nuovo Trattamento;
- all'aggiornamento conseguente alle modifiche dei Trattamenti.

Il Registro deve indicare, in particolare:

- nome e dati di contatto del Titolare;
- finalità del Trattamento;
- categorie di Interessati e di Dati trattati;
- categorie di terzi destinatari a cui i Dati possono essere eventualmente comunicati;
- eventuali trasferimenti di Dati verso paesi terzi ed indicazione delle adeguate garanzie;
- termini ultimi per la cancellazione (rispetto alle finalità del Trattamento);
- descrizione generale delle misure di sicurezza tecniche e organizzative.

3.2.2 Data Protection Impact Assessment (DPIA)

Ciascun Autorizzato al Trattamento di Dati Personali / Referente, in caso di avvio o modifica di un Trattamento dei Dati, informa preventivamente il Titolare e/o il Responsabile della Protezione dei Dati, provvedendo alla compilazione dell'apposita riga del Registro dei Trattamenti.

Qualora dal nuovo Trattamento possa emergere che esso presenti **rischi specifici per i diritti e le libertà degli interessati, in quanto effettuato per mezzo di nuove tecnologie, ovvero per il suo oggetto o le sue finalità**, il Titolare e/o il Responsabile della Protezione dei Dati (se nominato) richiede lo svolgimento di un "Data Protection Impact Assessment".

Nella propria valutazione, il Titolare/DPO terrà conto anche dei riscontri acquisiti all'esito delleinformative periodiche e specifiche.

L'Analisi d'Impatto, oltre che in occasione dell'avvio o della modifica di un Trattamento da cui possano derivare rischi per gli Interessati, secondo quanto testé indicato nella competenza del Titolare del trattamento, potrà essere disposta dallo stesso DPO, anche su base periodica nell'ambito

del Piano delle attività.

È comunque sempre richiesto lo svolgimento del Data Protection Impact Assessment nei casi seguenti:

- Dati Particolari ovvero Dati relativi a condanne penali e reati ovvero altre tipologie di Dati Personali che possano comportare potenziali rischi per i diritti e le libertà degli Interessati;
- decisioni automatizzate con conseguenze giuridiche o effetti significativi sulla persona, come ad esempio discriminazioni o esclusioni;
- monitoraggio sistematico di soggetti Interessati anche in aree pubbliche (es. videosorveglianza e geolocalizzazione);
- profilazione di uno o più soggetti Interessati;
- combinazioni di Dati Personali provenienti da diversi Trattamenti e/o da differenti Titolari e/o comunque provenienti da diverse banche dati;
- Dati Personali trattati su larga scala, ovvero relativi ad un elevato numero di soggetti Interessati o comprendenti enormi quantità di Dati Personali;
- Dati Personali relativi a dipendenti che non siano nelle condizioni di esprimere il consenso o opporsi al Trattamento (es. richieste di informazioni da parte dell'Autorità Giudiziaria e/o comunque da altre Autorità competenti, anche amministrative);
- utilizzo di soluzioni e tecnologie innovative che potrebbero implicare nuove forme di Trattamento di Dati Personali;
- eventuale trasferimento di dati personali verso Paesi Extra SEE.

In occasione della prima applicazione della presente procedura, ciascun Trattamento già in essere che rientra nella casistica sopra elencata dovrà essere oggetto di Data Protection Impact Assessment.

Il Data Protection Impact Assessment viene condotto dal Titolare, dal Responsabile del Trattamento e/o dall'Autorizzato Referente coinvolti, con il supporto eventuale del Responsabile della Protezione dei Dati, nonché con l'eventuale coinvolgimento di soggetti esterni specializzati, e deve tenere conto almeno dei seguenti elementi di analisi:

- una descrizione sistematica dei Trattamenti previsti (inclusi: natura, scopo, contesto e finalità del trattamento, categorie di Dati Personali e di Interessati, gli strumenti in uso per il Trattamento);
- un'analisi dei rischi per i diritti e le libertà degli Interessati (origine e natura dei rischi, impatti in caso di perdita di riservatezza, minacce per l'integrità e la disponibilità dei dati, probabilità e gravità dei rischi);
- una valutazione delle misure tecniche ed organizzative che contribuiscono a garantire la necessità e la proporzionalità del Trattamento (es. legittime e specifiche finalità, liceità del trattamento, minimizzazione dei dati, conservazione limitata, Informative, Consensi, rispetto dei diritti, individuazione dei Responsabili e degli Autorizzati, garanzie per l'eventuale trasferimento dei dati extra SEE).

3.2.3 Informativa sul Trattamento dei Dati Personali

Ogni qualvolta si intenda effettuare un Trattamento di Dati Personali, anche all'esito di un Data Protection Impact Assessment, nei casi in cui questo sia necessario, il Titolare è tenuto obbligatoriamente a fornire l'Informativa agli Interessati in merito ai loro diritti, fatti salvi i casi di esclusione previsti dalle disposizioni vigenti e di cui al successivo par. 4.2.5.

In caso di modifica delle finalità o delle modalità del Trattamento, oltre all'esecuzione del Data Protection Impact Assessment nei casi in cui esso sia necessario, deve sempre e comunque essere fornita all'Interessato una nuova Informativa.

Il Titolare del Trattamento che deve provvedere, anche tramite un suo Autorizzato, alla raccolta dei Dati Personali presso l'Interessato, deve preliminarmente predisporre, con il supporto del DPO, la relativa Informativa sul trattamento dei dati personali.

L'Informativa deve contenere le seguenti informazioni:

- i riferimenti del Titolare del Trattamento;
- i riferimenti del Responsabile della Protezione dei Dati;
- le finalità del Trattamento cui sono destinati i Dati Personali nonché la base giuridica del Trattamento;
- l'interesse connesso all'attività svolta dal Titolare del Trattamento in conformità alla legge;
- gli eventuali destinatari o le eventuali categorie di destinatari dei Dati Personali in caso di trasferimento;
- l'intenzione del Titolare del Trattamento di trasferire Dati Personali a un Paese terzo o a un'organizzazione internazionale;
- il periodo di conservazione dei Dati Personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- il diritto dell'Interessato di chiedere al Titolare l'accesso ai Dati Personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento o l'opposizione al loro Trattamento, oltre al diritto alla portabilità dei Dati;
- il diritto di revocare il Consenso in qualsiasi momento senza pregiudicare la liceità del Trattamento, la quale è basata sul Consenso prestato prima della revoca;
- il diritto di proporre reclamo all'Autorità Garante;
- l'indicazione se la comunicazione di Dati Personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'Interessato ha l'obbligo di fornire i Dati Personali nonché le possibili conseguenze della loro mancata comunicazione;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

A titolo esemplificativo, sono rilasciate Informative nei casi di seguito riportati:

- ai dipendenti e collaboratori all'atto dell'assunzione;
- ai fornitori e consulenti persone fisiche, all'atto della richiesta di offerta o comunque con l'emissione dell'ordine ovvero in caso di ogni attività di negoziazione e stipula di contratti di

approvvigionamento di lavori, servizi e forniture ovvero di prestazioni professionali;
- ai clienti e/o partner commerciali, al momento della raccolta dei Dati Personali (es. sottoscrizione del contratto).

Qualora l'acquisizione dei Dati Personali non avvenga direttamente presso l'Interessato (es. tramite banche dati o da parte di altro Titolare) sarà necessario, eccetto i casi di esclusione previsti dalle disposizioni vigenti e di cui al successivo par. 4.2.5, che il Titolare predisponga l'Informativa fornendo le informazioni di cui sopra e che la stessa sia trasmessa all'Interessato entro un termine ragionevole dall'ottenimento dei Dati Personali ma al più tardi entro un mese. In tali casi, l'Informativa deve contenere altresì la fonte da cui i Dati Personali sono acquisiti.

3.2.4 Consenso al Trattamento dei Dati Personali

Affinché un Trattamento di Dati Personali sia lecito è necessario che il suo avvio sia preceduto dall'Informativa all'Interessato secondo le modalità descritte nel paragrafo precedente e dall'acquisizione del relativo Consenso.

Detto Consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un Trattamento chiaramente individuato e se acquisito con un consenso separato (c.d. granulare) per ogni tipologia di trattamento.

In particolare, dovranno essere oggetto di separato e specifico consenso i trattamenti relativi ai fini di commercializzazione e marketing e i trattamenti di profilazione, la cessione a terzi, l'esportazione in altri Stati membri, oltre che i trattamenti che riguardano Dati Particolari, i quali dovranno essere sempre soggetti a consenso scritto ed esplicito. In caso di cessione a terzi per fini di marketing/commercializzazione dei dati, dovranno essere indicate le categorie merceologiche (o attività ATECO) delle tipologie di soggetti a cui i dati possono essere ceduti.

Qualora i dati debbano essere trasferiti al di fuori dell'Unione Europea e dello Spazio Economico Europeo, dovrà essere fatta una valutazione con il DPO della tipologia di consenso da richiedere.

Al fine di poter dimostrare l'inequivocabilità del Consenso, il Titolare deve assicurare che il Consenso sia prestato di regola per iscritto, con le modalità ed i mezzi consentiti dalla legge.

La documentazione del Consenso, espresso da parte dell'Interessato, deve essere allegata e conservata unitamente alla pratica relativa all'Interessato stesso. A tal proposito è compito del Titolare provvedere alla conservazione / archiviazione della documentazione del Consenso.

3.2.5 Casi di esclusione dall'obbligo di acquisire il Consenso

In conformità a quanto previsto dal Regolamento, non è necessaria la preliminare acquisizione del Consenso da parte dell'Interessato, tra gli altri, nei casi in cui il trattamento:
- riguardi dati raccolti e detenuti in base ad un obbligo di legge al quale è soggetto il Titolare;

- riguardi dati raccolti e detenuti dal Titolare in base ad un contratto di cui l'Interessato è parte;
- è necessario per l'esecuzione di obblighi derivanti dal contratto di lavoro o per l'acquisizione di informazioni precontrattuali attivate su richiesta dell'Interessato (es. curricula inviati al Titolare del Trattamento) ovvero per l'adempimento di un obbligo legale;
- riguardi dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;
- è finalizzato unicamente a scopi statistici o si tratta di dati anonimi;
- è necessario per la salvaguardia o l'incolumità fisica dell'Interessato o di un terzo;
- è necessario per far valere o difendere un diritto in sede relativi a condanne penali e reati.

3.2.6 Raccolta, utilizzo e conservazione dei Dati Personali

I Dati Personali trattati dal Titolare del Trattamento possono essere archiviati in banche dati informatiche o cartacee, comunque strutturate in modo da poter reperire le informazioni riferibili all'Interessato, nel rispetto delle regole e dei principi previsti dalla normativa e di seguito richiamati a titolo esemplificativo:

I Referenti e gli Autorizzati al trattamento hanno il compito di:

- utilizzare i Dati Personali esclusivamente per gli scopi del Trattamento che sono stati comunicati agli Interessati attraverso la relativa Informativa;
- mantenere sempre aggiornati e corretti i Dati Personali sulla base delle informazioni ricevute dall'Interessato;
- conservare i Dati Personali per un periodo di tempo non superiore agli scopi per i quali essi sono stati raccolti o successivamente trattati e comunque nel rispetto degli obblighi di legge.

3.2.7 Archivi cartacei e documentazione interna

Gli archivi contenenti gli atti e i documenti nei quali sono raccolti Dati Personali vengono sottoposti a controllo e custodia per tutto il tempo necessario al loro Trattamento, anche in relazione alla natura dei Dati Personali e alle possibili finalità di Trattamento stabilite nell'Informativa o comunque consentite dalle normative applicabili in materia.

I Referenti e gli Autorizzati dovranno custodire la documentazione interna negli appositi armadi provvisti di serratura ed avvertire tempestivamente le strutture interne competenti in caso di anomalie.

I Referenti e gli Autorizzati dovranno altresì controllare e custodire i relativi documenti impedendone l'accesso a persone non autorizzate. L'accesso delle persone ai predetti archivi deve essere comunque controllato (es. mediante apposito registro degli accessi).

3.2.8 Archivi informatici e strumenti tecnologici

Nel caso di Trattamento di Dati Personali con modalità informatiche, i Referenti e gli Autorizzati si attengono alle norme ed ai principi previsti negli strumenti normativi che disciplinano le regole di

utilizzo degli strumenti informatici da parte degli utenti e che descrivono le funzioni coinvolte nel processo di sicurezza informatica, cui si rinvia, ivi espressamente inclusi i regolamenti interni adottati.

Per il Trattamento di Dati Personali potranno essere utilizzati solo ed esclusivamente gli strumenti tecnologici messi a disposizione dal Titolare e/o in ogni caso specificamente approvati o autorizzati dallo stesso, anche per il tramite delle competenti funzioni interne.

Sono strumenti tecnologici in grado di trattare Dati Personali, a mero titolo di esempio non esaustivo: eventuali smartphone, tablet, personal computer e similari.

3.2.9 Comunicazione e diffusione dei Dati Personali

È vietata la comunicazione e la diffusione dei dati trattati dal Titolare del Trattamento sia quando è stata ordinata la cancellazione dei Dati Personali sia quando le finalità del Trattamento sono differenti da quelle per le quali essi erano stati raccolti.

Gli Autorizzati Referenti e gli Autorizzati, con il supporto dell'Amministratore di Sistema, devono adottare idonee misure di sicurezza per evitare che si verifichino ipotesi di comunicazione o diffusione dei Dati Personali trattati in mancanza del necessario Consenso dell'Interessato, ovvero in assenza delle cause previste dalle normative applicabili.

L'eventuale comunicazione o diffusione dei Dati Personali è ammissibile qualora l'Informativa predisposta contenga indicazione circa i destinatari o le categorie di destinatari ai quali i Dati Personali possono essere comunicati, oppure ove ciò sia previsto come obbligatorio ai sensi della normativa applicabile (ad esempio, per ordine dell'Autorità Garante e/o delle Autorità pubbliche competenti, nell'esercizio delle proprie funzioni).

3.2.10 Trasferimento dei Dati Personali all'estero

Il trasferimento dei Dati Personali all'estero è limitato alle sole attività ove sia espressamente necessario, ed è ammesso unicamente per le operazioni di Trattamento specificamente individuate ed all'interno dello Spazio Economico Europeo e/o di stati extra-SEE la cui normativa sulla protezione dei dati personali sia stata esaminata e ritenuta conforme e/o assimilabile nelle garanzie e nei principi e contenuti fondamentali a quella Italiana ed Europea dall'Autorità Garante, secondo la normativa vigente.

È espressamente vietato l'utilizzo di sistemi di memorizzazione online di dati informatici (es. sistemi cloud che consentono la memorizzazione o l'uso online di documenti) che non siano conformi a quanto previsto nel presente paragrafo 4.2 o che non siano stati espressamente e previamente esaminati dal Titolare o, per esso, dal DPO e ritenuti conformi.

3.3 DIRITTI DELL'INTERESSATO

L'Interessato, ossia il soggetto di cui si acquisiscono Dati Personali, ha la facoltà di esercitare alcuni diritti che possono riguardare le tipologie di Dati rispetto ai quali il Titolare effettua un Trattamento (es. finalità, tempistiche, destinatari, ecc.) oppure le modalità di gestione dei Dati stessi (es. portabilità, cancellazioni, rettifiche, ecc.).

L'esercizio dei diritti dell'Interessato prende avvio da una richiesta, da parte di quest'ultimo, con le modalità previste dalla legge e/o tramite la modulistica (anche telematica) predisposta dal Titolare, di concerto con il DPO, ove nominato.

Successivamente, il DPO ricevuta detta richiesta provvede a mezzo mail ad avvisare l'Autorizzato Referente competente.

L'Autorizzato, con il supporto dell'Amministratore di Sistema (per quanto attiene principalmente alle modalità di rettifica, cancellazione e portabilità dei Dati Personali) e del DPO, organizza la messa a disposizione dei Dati richiesti per fornire riscontro all'Interessato, al più tardi entro un mese dal ricevimento della richiesta.

Il DPO, sulla base delle verifiche svolte dal Titolare del Trattamento / Autorizzato Referente, fornisce idoneo riscontro, fermo restando che eventuale documentazione necessaria potrà essere materialmente trasmessa all'Interessato dal Titolare e/o dal Referente competente.

Il termine di un mese dal ricevimento della richiesta può essere prorogato fino a due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. In tal caso, il DPO informa l'Interessato di tale proroga e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

Il riscontro all'Interessato deve avvenire in forma scritta a mezzo mail da parte del DPO, acquisita la documentazione da parte del Titolare del Trattamento / Autorizzato Referente.

Ferme restando le formalità previste per la presentazione della richiesta e per il conseguente riscontro, l'Interessato potrà comunque rivolgersi al DPO per ogni chiarimento e supporto in merito all'esercizio dei propri diritti.

Nei casi in cui non si riesca ad adempiere nei termini indicati dalla legge o sia opportuno richiedere informazioni ulteriori, il Titolare del Trattamento / Autorizzato Referente deve darne immediata comunicazione all'Interessato.

Nel caso in cui il Titolare del Trattamento rilevi di non essere in possesso delle informazioni richieste e per la loro acquisizione è necessario svolgere un'attività che comporta una spesa, il Titolare del Trattamento si riserva il diritto di richiedere all'Interessato anche il rimborso dei costi che devono essere sostenuti.

Di seguito, si forniscono, informazioni in merito ai diritti esercitabili dall'Interessato e le connesse modalità operative per assicurarne il soddisfacimento.

3.3.1 Diritto di accesso

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 ottenerel'accesso ai Dati Personali e alle seguenti informazioni:

- le finalità del Trattamento;
- le categorie di Dati Personali in questione;
- 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;
- quando possibile, il periodo di conservazione dei Dati Personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- il diritto dell'Interessato di chiedere al Titolare del Trattamento la rettifica o la cancellazione dei Dati Personali o la limitazione del Trattamento o l'opposizione al Trattamento;
- il diritto di proporre reclamo all'Autorità Garante;
- qualora i Dati Personali non siano raccolti presso l'Interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione;
- tutti i riferimenti dei Responsabili e degli Autorizzati nominati ed in carica.

In tali casi, presentata la richiesta da parte dell'Interessato e fornito il riscontro da parte del DPO, il Responsabile del Trattamento fornisce una copia dei Dati Personali. In caso di ulteriori copie richieste dall'Interessato, può essere addebitato un contributo spese basato sui costi amministrativi.

3.3.2 Diritto di rettifica

L'Interessato ha il diritto di ottenere la rettifica o l'integrazione dei Dati Personali che ha già fornito al Titolare del Trattamento.

Pertanto, a seguito della richiesta da parte dell'Interessato e fornito il riscontro da parte del DPO, il Titolare del Trattamento, eventualmente per mezzo di un Referente o di unAutorizzato, provvedono alla rettifica o all'integrazione dei dati già in loro possesso.

3.3.3 Diritto alla portabilità

L'Interessato ha il diritto di richiedere la portabilità dei Dati Personali, che consiste:

- nella restituzione dei propri Dati forniti su un formato strutturato, di uso comune e leggibile da dispositivo automatico;
- se tecnicamente fattibile, nella trasmissione diretta dei Dati Personali da un Titolare del Trattamento all'altro, senza impedimenti da parte del Titolare del Trattamento che li ha forniti.

A tal fine, è necessario che per il Trattamento:

- sia stato effettuato sulla base del Consenso dell'Interessato o sia effettuato in esecuzione di un contratto;
- sia effettuato con mezzi automatizzati.

Qualora l'Interessato intenda esercitare tale diritto, il Titolare, il Referente o l'Autorizzato, con il supporto dell'Amministratore di Sistema, dovrà verificare la sussistenza dei presupposti necessari all'esercizio del Diritto. Pertanto, a seguito della richiesta da parte dell'Interessato e fornito il riscontro da parte del DPO, il Titolare, il Referente o l'Autorizzato provvederà a fornire copia dei Dati Personali direttamente all'Interessato ovvero ad altro Titolare, in conformità a quanto previsto nella richiesta/riscontro.

3.3.4 Diritto di limitazione al Trattamento

Il diritto di limitazione al Trattamento è esercitabile non solo in caso di violazione dei presupposti di liceità del Trattamento (quale modalità alternativa alla cancellazione dei dati stessi), bensì anche se l'Interessato chiede la rettifica dei Dati Personali (in questo caso la limitazione varrà in attesa di tale rettifica da parte del Titolare) o si oppone al loro trattamento (in questo caso la limitazione varrà in attesa della valutazione da parte del Titolare con il supporto del DPO, ove nominato).

Qualora l'interessato intenda esercitare tale diritto, il Titolare, il Referente o l'Autorizzato, con il supporto dell'Amministratore di Sistema, dovrà verificare la sussistenza dei presupposti necessari all'esercizio del diritto. Pertanto, a seguito della richiesta da parte dell'Interessato e fornito il riscontro da parte del DPO, il Titolare del Trattamento provvederà alla limitazione dell'utilizzo dei Dati Personali.

3.3.5 Diritto di opposizione ad un Trattamento

L'Interessato ha il diritto di opporsi al Trattamento dei Dati Personali che lo riguardano compresa la profilazione, salvo che il Titolare 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 relativi a condanne penali e reati.

Pertanto, a seguito della richiesta dell'Interessato e fornito il riscontro da parte del DPO, il Titolare del Trattamento, eventualmente per mezzo di un Referente o un Autorizzato, provvede alla cancellazione dei Dati Personali.

3.3.6 Diritto alla cancellazione (diritto all'oblio)

L'Interessato ha diritto di ottenere la cancellazione dei Dati Personali in presenza dei seguenti motivi:

- i Dati Personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti (cancellazione automatica ovvero senza richiesta dell'Interessato);
- l'Interessato revoca il consenso sulla base del quale il Trattamento è stato effettuato o vengono meno gli altri presupposti del Trattamento (es. venir meno degli obblighi di legge o di contratto o della base giuridica);
- l'Interessato si oppone al Trattamento e non sussiste alcun motivo legittimo del Titolare;
- i Dati Personali sono trattati illecitamente;
- i Dati Personali devono essere cancellati per adempiere un obbligo legale.

Qualora l'Interessato intenda esercitare tale diritto, il Titolare, l'Autorizzato Referente o

l'Autorizzato, con il supporto dell'Amministratore di sistema, dovrà verificare la sussistenza dei presupposti necessari all'esercizio del diritto. Pertanto, a seguito della richiesta dell'Interessato e fornito il riscontro da parte del DPO, il Titolare del Trattamento, eventualmente per mezzo di un Referente o un Autorizzato, provvede alla cancellazione dei Dati.

3.4 MISURE DI SICUREZZA

Per il Trattamento di Dati Personali su supporti informatici, l'Amministratore di Sistema, in collaborazione con gli Autorizzati e con il DPO, predispone ed aggiorna le misure di sicurezza informatica, sulla base dell'analisi dei rischi e della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al Trattamento dei Dati stessi.

In particolare, l'Amministratore di Sistema predispone, anche mediante procedure e istruzioni operative e connessa modulistica:

- l'analisi dei rischi che possono incombere sui Dati Personali, con eventuali piani di rientro a fronte di criticità identificate e correlate azioni di miglioramento;
- le misure da adottare per garantire l'integrità e la disponibilità dei Dati rilevanti ai fini della loro custodia e accessibilità (a titolo esemplificativo: gestione di file e cartelle condivise, postazioni inattive, salvataggi dei Dati, protezione contro virus, utilizzo di supporti esterni di memorizzazione);
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei Dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi, con il supporto da parte del DPO, gli Autorizzati Referenti e gli Autorizzati al Trattamento, allo scopo di renderli edotti dei rischi che incombono sui Dati, delle misure disponibili per prevenire eventi dannosi e delle modalità per aggiornarsi sulle misure minime da adottare;
- la descrizione dei criteri necessari per garantire l'adozione delle misure minime di sicurezza in caso di Trattamenti di Dati Personali affidati all'esterno.

Le postazioni di lavoro costituiscono lo strumento per mezzo del quale il i Referenti egli Autorizzati fruiscono dei servizi informatici ed accedono alle risorse informative del Titolare del Trattamento. Dalle singole postazioni di lavoro, in base anche alle loro caratteristiche tecniche, sarà possibile accedere:

1. ai dati e programmi gestiti sui sistemi centrali (server), mediante la connessione ad essi con sistemi di rete locale (LAN) o altra modalità (wi-fi, remoto);
2. ai dati e programmi memorizzati localmente sulla postazione di lavoro (modalità "*stand alone*").

Per ciascuna delle suddette modalità vengono descritte di seguito le misure minime di sicurezza da adottare.

3.4.1 Protezione dei Dati Personali gestiti mediante elaboratori connessi in rete

Il Trattamento dei Dati Personali (dall'accesso ad ogni attività di utilizzo, comprese le operazioni di modifica, estrazione e cancellazione), memorizzati e gestiti sui sistemi centrali e connessi alla rete informatica, devono essere protetti da meccanismi di *User-ID e password* assegnati a ciascun Autorizzato.

I suddetti meccanismi devono consentire l'identificazione del Referente/Autorizzato, il controllo dell'autorizzazione di accesso e Trattamento dei Dati, nonché la registrazione e la tracciabilità di tutte le operazioni e attività svolte sui Dati medesimi.

3.4.2 Protezione dei Dati Personali gestiti localmente su personal computer

Il Trattamento dei Dati Personali (dall'accesso ad ogni attività di utilizzo, comprese le operazioni di modifica, estrazione e cancellazione), memorizzati e gestiti localmente, devono essere effettuati, tramite l'utilizzo di *User-ID e password* allo scopo di impedire l'accesso a persone non autorizzate. Con il termine "localmente" si intende il Trattamento dei Dati effettuato tramite *personal computer* nel caso in cui i Dati sono memorizzati sul disco fisso del *personal computer* stesso (modalità "stand-alone"), ad uso esclusivo dell' Autorizzato Referente/Autorizzato.

Vengono assimilati a tale modalità di lavoro i Trattamenti effettuati in una delle seguenti configurazioni:

- i Dati sono memorizzati su una porzione di disco del *server* di rete messa a disposizione dell'Autorizzato come estensione delle risorse del suo *personal computer*;
- i Dati sono memorizzati in modo condiviso su una postazione di lavoro (server) connessa in rete locale ad altri *personal computer* (*client*) dai quali possono essere effettuati l'accesso ed il Trattamento dei Dati stessi (es. applicazioni).

In detti casi la protezione dei Dati Personali memorizzati e gestiti localmente può essere effettuata o mediante digitazione obbligatoria di *User-ID e password* all'atto dell'accensione di un *personal computer* ovvero essere prevista a livello di singola applicazione o mediante entrambe le modalità.

Ai fini dell'effettiva applicazione della presente procedura, l'Amministratore di Sistema predispone un piano di implementazione delle misure di sicurezza in linea con le disposizioni sopra indicate ed in conformità ai requisiti di cui all'art. 32 del GDPR, dettagliando le modalità e le tempistiche di attuazione.

5. VERIFICHE, FLUSSI INFORMATIVI E SEGNALAZIONI

5.1 VERIFICHE

Nell'ambito del Piano delle attività, il Responsabile della Protezione dei Dati provvede alla realizzazione di verifiche relativamente all'adeguatezza e all'osservanza delle disposizioni della

presente procedura e in generale in materia di protezione dei dati personali, ivi specificamente incluse eventuali verifiche sulla correttezza dell'operato degli Autorizzati.

Il Responsabile della Protezione dei Dati, autonomamente o anche avvalendosi delle competenti funzioni interne (in particolare: audit e IT) o di consulenti esterni, potrà:

- richiedere documentazione o svolgere interviste afferenti i Trattamenti dei Dati Personali svolti da parte degli Autorizzati Referenti e Autorizzati;
- chiedere informazioni in merito a segnalazioni ricevute da parte di Responsabili, Referenti, Autorizzati o Interessati circa una qualsiasi violazione dei Dati Personali ed effettuare i necessari approfondimenti;
- predisporre la documentazione relativa alle attività condotte concordando con gli Autorizzati Referenti / Autorizzati le eventuali necessarie azioni correttive da avviare.

In particolare, le verifiche saranno condotte nelle aree esposte ai rischi e comunque in quelle rispetto ai quali sono stati nominati gli Autorizzati Referenti, tenendo conto dei seguenti elementi:

- rilevanza dei Trattamenti (in termini di numerosità e tipologia di Dati Personali) svolti da ciascun Referente;
- eventuali indicazioni derivanti da altre funzioni interne ovvero dalle notizie acquisite tramite i flussi informativi;
- richieste ad hoc ricevute dal Titolare e dai Responsabili del Trattamento.

Delle verifiche e degli eventuali rilievi e raccomandazioni per il miglioramento, il Responsabile della Protezione dei Dati Personali, ove nominato, dà conto nell'ambito dei propri periodici rapporti al Titolare.

5.2 FLUSSI INFORMATIVI E SEGNALAZIONI VERSO IL DPO O VERSO IL TITOLARE

Gestione delle segnalazioni

A fronte della segnalazione ricevuta, il Titolare, sentito il Responsabile della Protezione dei Dati, verifica la rilevanza e attendibilità dei fatti riferiti anche con il supporto delle funzioni interne competenti e/o di soggetti esterni.

Dopo avere esaminato la segnalazione, qualora risulti fondata la violazione delle disposizioni normative o procedurali, anche interne, i Titolare e/o il DPO, ove nominato, d'intesa con il Titolare, deve:

- valutare i comportamenti rilevati, anche ai fini del procedimento disciplinare, raccogliendo tutta la documentazione e le informazioni necessarie;
- ove necessario, valutata la presenza di rischi – anche potenziali – per le attività di Trattamento, avviare le procedure di Data Protection Impact Assessment di cui al par. 4.2.2;
- ove necessario, avviare l'attività di notifica di violazione prevista nel par. 6.1;
- in ogni caso, attivare i Referenti e le altre funzioni competenti affinché siano poste in essere tutte le azioni necessarie a regolarizzare la posizione dei Dati Personali coinvoltinell'evento, se del caso interrompendo – anche temporaneamente – le attività di Trattamento degli stessi.

5.3 FLUSSI INFORMATIVI DAL DPO AL TITOLARE

Sulla base dei flussi informativi trasmessi dagli Autorizzati, il DPO, ove nominato, trasmette al Titolare un'informativa nella quale fornisce un resoconto sulle attività svolte nel periodo di riferimento.

Detta relazione fornisce indicazioni sullo svolgimento del Piano delle attività e sugli adempimenti svolti ai sensi della presente procedura, in particolare con riguardo alle seguenti tematiche:

- evoluzioni normative, giurisprudenziali e delle prassi applicative (es. linee guida delle Autorità Garanti europea e nazionale) in materia di protezione dei dati personali;
- eventuali aggiornamenti sulle nomine (Responsabili, Autorizzati, Amministratori di Sistema) e altre modifiche alle strutture organizzative aventi un impatto suiTrattamenti;
- eventuali modifiche di maggior rilievo nella gestione dei Dati, quali risultanti dai Data Protection Impact Assessment;
- esiti delle verifiche svolte, con la descrizione delle principali criticità, delle relative azioni correttive e del loro stato di avanzamento;
- informazioni in merito alle informative ricevute dai Responsabili e alle segnalazioni ricevute dagli Interessati;
- informazioni sulle campagne di comunicazione e sulle iniziative di formazione delle figure preposte e di divulgazione delle regole in materia di Privacy con il personale;
- eventuali rapporti intrattenuti con le Autorità Garanti europea e nazionale o con altre Autorità competenti (richieste di informazioni, collaborazione ad indagini, segnalazione di violazioni/illeciti/irregolarità);
- ulteriori aspetti di rilievo ritenuti necessari (es. proposte di modifica delle procedure o dell'organizzazione, attività di miglioramento).

6. RAPPORTI CON L'AUTORITÀ GARANTE

6.1 NOTIFICA DI VIOLAZIONE (DATA BREACH NOTIFICATION)

In caso di violazione dei Dati Personali (es. distruzione accidentale o perdita dei dati, divulgazione, modificazione, copia o rimozione in assenza di autorizzazione, ecc.) il Responsabile del Trattamento e/o il Referente e/o l'Autorizzato che ne apprende notizia informa tempestivamente il DPO oppure direttamente il Titolare di dette violazioni.

Salvo che sia improbabile che la violazione dei Dati Personali possa rappresentare un rischio per i diritti e le libertà dell'Interessato, il Titolare del Trattamento, in accordo con il DPO, procede a notificare la violazione dei Dati Personali senza ingiustificato ritardo all'Autorità Garante, possibilmente entro 72 ore dal momento in cui ne è giunto a conoscenza.

La notifica all'Autorità Garante deve contenere i seguenti elementi minimi:

- descrivere la natura della violazione dei Dati Personali, le categorie e il numero approssimativo di Interessati;
- comunicare i riferimenti del Responsabile della Protezione dei Dati o altro riferimento per

l'ottenimento di eventuali informazioni ulteriori (in particolare il Responsabile nella cui area si è verificata la violazione);
- descrivere le possibili conseguenze della violazione;
- descrivere le misure adottate per porre rimedio alla violazione o quelle che potrebbero essere poste in essere per mitigarne gli effetti.

Successivamente alla notifica, sarà necessario acquisire il parere dell'Autorità Garante che potrà comportare la necessità anche di fornire informazioni all'Interessato in merito alla violazione dei Dati Personali. La notifica all'Interessato in merito alla violazione non sarà necessaria, qualora l'Autorità Garante valuti soddisfatta una delle seguenti condizioni:

- siano state messe in atto misure in grado di rendere incomprensibili i Dati Personali a chiunque vi possa accedere a seguito della violazione;
- le misure di sicurezza messe in atto siano tali da scongiurare che vi possano essere rischi elevati per i diritti dell'Interessato;
- la comunicazione all'Interessato richiederebbe sforzi (anche economici) sproporzionati.

Tutte le notifiche o comunicazioni effettuate in relazione alle procedure di cui al presente par. 6 sono archiviate per essere eventualmente rese disponibili in caso di accertamenti o verifiche dell'Autorità Garante.

6.2 CONSULTAZIONE CON L'AUTORITÀ GARANTE

Oltre all'obbligo di notifica di cui al paragrafo precedente e/o gli altri casi in cui la consultazione è obbligatoria, il Responsabile della Protezione dei Dati e/o il Titolare, qualora lo ritenga necessario, potrà consultare l'Autorità Garante per la Protezione dei Dati Personali per acquisire pareri o formulare interpelli.

In tali casi, il Referente o l'Autorizzato coinvolto nell'attività fornisce al DPO e/o al Titolare ogni informazione necessaria per eseguire l'interpello.

7. DIFFUSIONE DELLA MODULISTICA E ARCHIVIAZIONE

La Modulistica standard da utilizzare obbligatoriamente per la gestione degli adempimenti, è diffusa e resa disponibile mediante specifica comunicazione email ai dipendenti nonché disponibile su cartella presente nel pc di ogni dipendente.

In particolare, il Titolare e/o il Responsabile della Protezione dei Dati cura l'aggiornamento della presente procedura e della modulistica necessaria a garantire il corretto svolgimento degli adempimenti normativi e/o definiti nella procedura stessa.

Tutti gli Autorizzati Referenti e gli Autorizzati sono tenuti all'utilizzo corretto della modulistica disponibile nonché a garantire un'adeguata ed ordinata archiviazione di tutti i moduli predisposti e compilati da mettere a disposizione del Responsabile della Protezione dei Dati, ove nominato (per

verifiche interne) e/o dell'Autorità Garante (per verifiche esterne).

8. SISTEMA SANZIONATORIO

Il procedimento di applicazione delle sanzioni, viene attivato conseguentemente alla violazione delle norme in materia di protezione dei Dati Personali da parte di dipendenti, sia in relazione all'esercizio delle proprie mansioni sia in conseguenza delle attività di eventuali soggetti esterni di cui si avvalgono, fermo restando che violazioni delle disposizioni in materia di protezione dei dati personali da parte di Autorizzati Referenti o Autorizzati possono comportare l'adozione di determinazioni per la tutela contrattuale o extracontrattuale in ogni opportuna sede.

Le violazioni della presente procedura e delle disposizioni in materia di protezione dei dati personali, oltre a costituire oggetto di eventuali obblighi informativi verso l'Autorità Garante, devono comunque essere prontamente segnalate al Titolare e/o al DPO, il quale provvederà a riferire al Titolare e/o ai competenti organi del Titolare del Trattamento per la valutazione dei profili disciplinari, ove da questa ritenuti applicabili.

Si segnala, per opportuna conoscenza, che il Regolamento prevede, in caso di violazioni della normativa sulla protezione dei Dati Personali ivi codificata, la possibilità, per l'Autorità Garante, di irrogare, a seguito del compimento della più opportuna attività ispettiva ed istruttoria in relazione ad abusi, illeciti e/o violazioni inerenti il Trattamento di Dati Personali, sanzioni di ingente entità (sino a 20.000.000 di Euro, o al 4% del fatturato del gruppo societario, ove maggiore); per tale ragione, si raccomanda di seguire le procedure descritte nel presente documento con la massima diligenza e perizia.