MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

SIPAGA BISALTA SpA

Prima Emissione / Revisione			
Prima emissione 00			16/10/2025
	Responsabili	**Formalizzazione**	**Data**
Redazione	RAM		16/10/2025
Approvazione	CDA		12/11/2025

PARTE GENERALE

PARTE SPECIALE

PARTE GENERALE

1. IL REGOLAMENTO UE 2016/679 (GDPR)

1.1 L'ADEGUAMENTO DELLA NORMATIVA NAZIONALE

Il Regolamento UE n. 2016/679, *General Data Protection Regulation* (di seguito anche "**Regolamento**" o "**GDPR**") è un atto di diritto dell'Unione Europea attraverso il quale la Commissione Europea ha inteso rafforzare e unificare la protezione dei dati personali entro i confini dell'Unione Europea (UE).

Il Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, entrato in vigore il 24 maggio 2016 e direttamente applicabile all'interno degli Stati membri dal 25 maggio 2018, ha introdotto una serie di obblighi finalizzati a garantire lo svolgimento di lecite e corrette operazioni di trattamento di dati personali da parte delle organizzazioni, in qualità di Titolari e/o Responsabili del trattamento.

In Italia il processo di adeguamento al GDPR è stato condotto attraverso l'adozione del Decreto Legislativo 10 agosto 2018, n. 101, in vigore dal 19 settembre 2018, il quale è intervenuto sul preesistente D.lgs. 196/2003 – c.d. Codice Privacy - mediante congiunti interventi integrativi, modificativi e di abrogazione.

I dati soggetti al GDPR sono i dati personali, ossia i "dati identificativi" come quelli anagrafici e di contatto e i dati sensibili/particolari, come quelli relativi alla salute o alle opinioni politiche e all'appartenenza sindacale.

In generale, può essere definito dato personale qualunque informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente, ossia riferita a persone fisiche e/o ditte individuali (i cosiddetti "**Interessati**"). I dati personali possono essere trattati dal soggetto Titolare del trattamento, ossia 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. Il Titolare deve a sua volta nominare Responsabili esterni ed interni del trattamento, che trattano i dati personali per conto del Titolare e anche soggetti Autorizzati al trattamento, ossia chiunque agisca sotto l'autorità del Titolare o del Responsabile del trattamento, che sia da quest'ultimo istruito e che abbia accesso ai dati personali oggetto del trattamento.

Il Regolamento si applica ai dati dei residenti nell'Unione Europea e anche a imprese ed enti, organizzazioni in generale, con sede legale fuori dall'UE che trattano dati personali di residenti nell'Unione Europea. Si precisa pertanto che devono adeguarsi alla normativa tutte le imprese, le organizzazioni e le Pubbliche Amministrazioni presenti negli stati membri dell'Unione Europea (indipendentemente dal fatto che il trattamento sia effettuato in UE), ma anche società extra UE che offrono servizi o prodotti a persone fisiche nel territorio dell'UE o che semplicemente monitorano il comportamento di soggetti all'interno dell'Unione.

L'adeguamento ai requisiti previsti dal GDPR comprende, tra le altre attività di *privacy compliance*, l'adozione e l'efficace ed effettiva attuazione di un "*Modello Organizzativo in Materia di Protezione dei Dati Personali*" (di seguito anche "**Modello Organizzativo Privacy**" o "**MOP**") che consenta alle imprese, enti ed organizzazioni, cui si applica il Regolamento, di:

(i) predisporre un sistema di controllo idoneo a prevenire i rischi privacy relativi ai dati personali, come sopra identificati e successivamente valutare i controlli esistenti, in termini di adeguatezza ai requisiti previsti dal GDPR ed effettiva operatività degli stessi;
(ii) gestire tempestivamente possibili criticità;
(iii) dare evidenza del sistema di controllo implementato evitando l'imputazione di responsabilità e delle sanzioni previste.

2. I PRINCIPI GENERALI E LE REGOLE PER IL TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati personali deve essere effettuato nel rispetto dei seguenti principi generali:

- **il diritto alla protezione del dato personale**, secondo il quale ogni individuo ha il diritto che il

trattamento dei suoi dati personali avvenga, secondo modalità che assicurino un elevato livello di tutela, nel rispetto dei suoi diritti e libertà fondamentali, nonché della sua dignità, con particolare riferimento alla riservatezza e all'identità personale;

- **il principio di liceità e correttezza**, che prescrive al soggetto che agisce sui dati personali la conformità alla legge del trattamento posto in essere e la trasparenza per l'interessato della raccolta e delle altre operazioni, vietando artifizi e raggiri. I dati personali trattati in violazione della normativa in materia protezione dei dati personali non possono essere utilizzati;
- **il principio di finalità**, secondo cui la raccolta dei dati deve essere collegata alla finalità perseguita, che deve essere legittima, determinata e non incompatibile con l'impiego dei dati;
- **il principio di necessità nel trattamento dei dati e di minimizzazione del loro utilizzo**, che impone che la raccolta e il trattamento di dati vada effettuato limitatamente alle sole informazioni necessarie all'attività, in modo da ridurre al minimo l'utilizzo di dati personali e di dati identificativi. Infatti, laddove le stesse finalità possano essere perseguite anche senza l'uso di dati personali, il trattamento deve riguardare solo dati anonimi oppure deve essere posto in essere adottando opportune modalità che permettano di identificare l'interessato solo in caso di necessità;
- **il principio di proporzionalità**, che prevede altresì di verificare, in ogni fase del trattamento, se le singole operazioni siano in concreto pertinenti e non eccedenti le finalità perseguite;
- **il principio di tutela dell'integrità del dato**, secondo il quale i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di adeguate misure tecniche ed organizzative, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- **il principio di accountability o di responsabilizzazione**, sulla base del quale tutti i dati devono essere trattati dal Titolare in modo responsabilizzato. Il Titolare deve quindi dimostrare, per ciascun trattamento, di aver agito in conformità alle disposizioni del GDPR. L'approccio metodologico da applicarsi al fine di garantire l'accountability è un approccio "*risk based*", ovvero l'approccio basato sulla valutazione del rischio del trattamento, che deve essere adottato e dimostrato da parte delle imprese, enti, o organizzazioni è di tipo proattivo, e non più reattivo, con focus su obblighi e comportamenti finalizzati a prevenire in modo effettivo il possibile evento di danno. Il rischio inerente al trattamento è da intendersi come rischio per la sicurezza dei dati e come rischio di impatti negativi sulle libertà e i diritti degli interessati. Tali impatti devono essere analizzati attraverso un apposito processo di valutazione (es. *Risk e Privacy Impact Assessment*) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) da adottare per mitigare tali rischi. L'approccio metodologico "*risk based*" deve quindi seguire logiche di *risk assessment* e *risk management*, al fine di valutare e ridurre il rischio per i diritti e le libertà dei soggetti dei dati e individuare le misure tecniche e organizzative idonee a garantire un adeguato livello di sicurezza;
- **Privacy by Design**, che sottende la necessità di prevedere, già in fase di progettazione del trattamento dati e dei sistemi informatici e applicativi, l'adozione di logiche di minimizzazione del trattamento e di disegno dello stesso sin dall'origine in linea coi principi in esame. Ogni titolare deve quindi assicurare che i sistemi informatici, prodotti e/o servizi offerti che prevedono il trattamento di dati personali nonché ogni progetto avviato siano, per impostazione predefinita, protetti da adeguate misure di sicurezza e garantiscano il più ampio rispetto dei diritti e delle libertà degli interessati in ottemperanza alla normativa in materia di protezione dei dati personali, senza che sia richiesto a questi ultimi alcun ulteriore intervento;
- **Privacy by Default** che implica l'implementazione da parte dell'organizzazione di un processo che preveda e disciplini le modalità di acquisizione, trattamento, protezione e modalità di diffusione dei dati personali, limitando la raccolta dei dati esclusivamente a quei dati personali realmente necessari per la realizzazione delle finalità perseguite, in ottemperanza al principio di

minimizzazione dei dati, e determinando sin dall'origine il periodo per il quale i dati personali raccolti dovranno essere conservati;

- **Consenso**, che deve essere esplicitamente prestato per ogni trattamento effettuato, ove non operino le esenzioni di legge. A tal proposito, se la richiesta per ottenere il consenso dagli interessati viene inserita nell'ambito di altre dichiarazioni essa va distinta e formulata con linguaggio semplice e chiaro. Condizione di validità del consenso è che le finalità per cui viene richiesto siano esplicite, legittime, adeguate e pertinenti. Nel caso in cui il consenso al trattamento dei dati personali per una o più specifiche finalità riguardi i minori, il GDPR richiede al Titolare del trattamento la verifica documentata dell'età del minore e, laddove necessario sulla base dell'età del minore, del consenso al trattamento da parte di un genitore o da chi eserciti la responsabilità genitoriale. I Titolari del trattamento dei dati devono essere in grado di dimostrare che l'interessato abbia prestato il consenso (i.e. principio "opt-in") e il consenso possa essere ritirato o modificato;
- **Data Breach**, definito come qualsiasi attività che comporti la distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Nei casi di violazione dei dati, accesso abusivo o, comunque, perdita degli stessi, i Titolari dei trattamenti saranno obbligati, entro 72 ore, ad avvisare l'Autorità di Controllo e, nei casi di particolare gravità, anche i diretti interessati, informando in relazione alle possibili conseguenze, alle misure adottate per rimediare o ridurre l'impatto del danno e ai dati di contatto degli organi e delle figure aziendali che vigilano sulla gestione e protezione del trattamento di dati personali in conformità alla legge;
- **Diritti degli interessati**, che includono tra l'altro:
  (i) diritto di accesso, che prevede il diritto di accedere e/o richiedere quali dati personali siano oggetto di trattamento con indicazione, ad esempio, del periodo di conservazione previsto o i criteri per definire tale periodo, nonché delle garanzie applicate in caso di trasferimento dei dati verso Paesi terzi;
  (ii) diritto alla cancellazione (diritto all'oblio), che prevede il diritto dell'interessato alla cancellazione dei propri dati personali ove non sussistano obblighi di legge o interessi prevalenti del Titolare, nonché l'obbligo per il Titolare o il Responsabile del trattamento di informare della richiesta di cancellazione altri Titolari che trattano i dati personali da cancellare, dando comunicazione all'interessato, dietro richiesta del medesimo, dei destinatari a cui ha trasmesso la sua richiesta di cancellazione;
  (iii) diritto di limitazione, che prevede, in caso di violazione dei presupposti di liceità del trattamento, la richiesta di limitazione del trattamento, in attesa della valutazione del Titolare, o di richiesta di rettifica dei dati presentata dall'interessato;
  (iv) diritto alla portabilità dei dati, che si applica ai soli dati automatizzati trattati con il consenso dell'interessato o sulla base di un contratto con lo stesso e forniti al Titolare dall'interessato medesimo, nei casi in cui lo stesso abbia la necessità di trasferirli ad un altro Titolare, laddove tecnicamente possibile;
- **Trasferimento dati extra UE**: Il GDPR vieta il trasferimento verso Paesi situati al di fuori dell'UE o a organizzazioni internazionali se effettuato in assenza di adeguati standard di tutela. Al contrario, invece, è permesso in caso di presenza di adeguate garanzie come clausole contrattuali tra Titolari autorizzate dal Garante, accordi e provvedimenti vincolanti tra autorità pubbliche amministrative e giudiziarie, clausole tipo adottate dal Garante, adesione a codici di condotta e/o meccanismi di certificazione. È inoltre permesso il trasferimento oltre UE in caso di decisioni di adeguatezza della Commissione UE (es. «*Privacy Shield EU/USA*», Svizzera, Argentina, Australia, Canada, ecc.), norme vincolanti di impresa (*Binding Corporate Rules* – «*BCR*») e casi in deroga (consenso informato dell'interessato, necessità per esecuzione adempimenti contrattuali e precontrattuali, interesse pubblico, diritto di difesa, interessi vitali, dati tratti da registro pubblico, ecc.);
- **Data Protection Officer**, definito ai sensi del Regolamento come il Responsabile della Protezione

dei dati personali o *Data Protection Officer* (DPO), la cui nomina è:

- obbligatoria ove:
  a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
  b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
  c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10".
- facoltativa negli altri casi, al fine di fornire consulenza ed assistenza giuridica e tecnica specialistica sulle questioni afferenti alla *data protection*[1].

Con riguardo all'attribuzione degli specifici compiti contemplati dal Regolamento, il DPO deve avere una serie di requisiti (a titolo esemplificativo, competenze giuridiche, competenze tecniche e di security) che consentano allo stesso di operare un *risk assessement*, ovvero valutare i rischi e fornire pareri su temi IT/Security ai fini dell'applicazione delle soluzioni e delle misure informatiche di sicurezza più adeguate. Svolge un ruolo di attivatore e, a suo carico, può rinvenirsi un dovere di impulso anche rispetto al Titolare e al Responsabile del trattamento che rimanga inattivo, violando il Regolamento. Secondo quanto previsto dell'art. 39 del GDPR, il DPO è autorizzato ad attribuire le responsabilità, sensibilizzare e formare il personale aziendale e chiunque sia coinvolto nelle attività di gestione dei trattamenti dei dati e nelle connesse attività di controllo, stabilendo chi e in quale misura, all'interno dell'impresa, ente o organizzazione, deve rispondere di eventuali comportamenti non conformi alle procedure interne di gestione dei dati. Il DPO supporta il Titolare nella tenuta del Registro dei trattamenti e fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati, sorvegliandone lo svolgimento ai sensi dell'articolo 35 del GDPR. Coopera, inoltre, con l'Autorità di controllo e funge da punto di contatto con la medesima per questioni connesse al trattamento dei dati;

- **Misure tecniche ed organizzative adeguate**, tra cui Informative, nomine, formazione ecc. e soprattutto procedure interne che formalizzino nell'ambito delle stesse adeguati controlli imposti dal GDPR e della concreta realizzazione di un sistema di compliance adeguato ad evitare un trattamento illecito dei dati personali e in grado di dimostrare che l'organizzazione aziendale ha proattivamente adottato e attuato tutti i presidi previsti dal Regolamento.

3. RESPONSABILITÀ

Il trattamento dei dati personali in violazione della normativa può dare luogo ad una responsabilità di carattere civile e/o penale e/o amministrativa, ovvero anche cumulativa in relazione ad un fatto unico.

In ambito civile, può legittimare una richiesta al risarcimento per danni da parte del soggetto leso, come previsto dal Codice civile ed in particolare dall'art. 2050 c.c., secondo il quale chiunque, sia esso persona fisica o persona giuridica, cagiona un danno ad altri per effetto del trattamento di dati personali e non dimostri di aver

[1] Il Garante della protezione dei dati personali, nelle sue FAQ sul DPO, prevede che "*nei casi diversi da quelli previsti dall'art. 37, par. 1, lettere b) e c), del GDPR, la designazione del DPO non è obbligatoria (ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale o comunque che non effettuano trattamenti su larga scala; amministratori di condominio; agenti, rappresentanti e mediatori non operanti su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti – a tale ultimo riguardo, cfr. anche considerando 97 del GDPR, in relazione alla definizione di attività "accessoria"). In ogni caso, resta comunque raccomandata, anche alla luce del principio di accountability che permea il GDPR, la designazione di tale figura (v., in proposito, WP 243, cit., par. 1)*".

adottato misure idonee ad evitarlo, è tenuto al risarcimento del danno medesimo.

La responsabilità legata al trattamento dei dati personali rientra infatti nel concetto di responsabilità per esercizio di attività pericolose, secondo il quale - ai sensi dell'art. 2050 c.c. sopra richiamato - "chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati è tenuto al risarcimento se non prova di avere adottato tutte le misure idonee ad evitare il danno".

Il concetto di responsabilità sopra definito, già contemplato dalla normativa in materia di privacy, si configura a prescindere dal comportamento colposo o doloso dell'autore, il quale, in virtù di un'inversione dell'onere della prova, per esimersi dalla responsabilità a suo carico, deve dare la dimostrazione di una prova liberatoria, ovvero di avere adottato tutte le misure atte ad evitare il danno avvenuto. Spetta a colui che ha subito il danno fornire la prova del danno medesimo e la dimostrazione del rapporto di causalità tra l'attività pericolosa esercitata ed il danno. I danni risarcibili possono essere di natura sia patrimoniale che non patrimoniale, intendendosi in quest'ultimo caso quei danni, liquidati in via equitativa da parte del giudice, derivanti dalla sofferenza fisica e/o morale del danneggiato.

Con riguardo alla responsabilità penale, le fattispecie criminose che assumono maggior rilevo riguardano il reato di accesso abusivo ad un sistema informatico o telematico (art. 615 ter Codice Penale), il reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater Codice Penale), nonché i reati previsti dal D.lgs. 196/2003 Codice in materia di protezione dei dati personali – c.d. Codice Privacy – come modificato dal D.lgs. 101/2018, e in particolare l'art. 167 - Trattamento illecito di dati, l'art. 167 bis - Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala, l'art. 167 ter - Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala, l'art. 168 - Falsità nelle dichiarazioni e notificazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante, l'art. 170 - Inosservanza di provvedimenti del Garante e l'art. 171 - Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori.

Con riguardo, infine, alla responsabilità amministrativa, il Regolamento stabilisce sanzioni amministrative che vanno inflitte, in funzione delle circostanze di ogni singolo caso, tenendo in debito conto i seguenti elementi: a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito; b) il carattere doloso o colposo della violazione; c) le misure adottate dal Titolare del trattamento o dal Responsabile del trattamento per attenuare il danno subito dagli interessati; d) il grado di responsabilità del Titolare del trattamento o del Responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto; e) eventuali precedenti violazioni pertinenti commesse dal Titolare del trattamento o dal Responsabile del trattamento; f) il grado di cooperazione con l'Autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; g) le categorie di dati personali interessate dalla violazione; h) la maniera in cui l'Autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il Titolare del trattamento o il Responsabile del trattamento ha notificato la violazione; i) il rispetto di tali provvedimenti; j) l'adesione ai codici di condotta o ai meccanismi di certificazione; e k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

In caso di violazioni della normativa in vigore sono passibili di responsabilità e quindi tenuti al risarcimento il Titolare del trattamento ed il Responsabile del trattamento. Il Titolare deve risarcire qualsiasi danno a lui imputabile che abbia cagionato a causa della violazione del Regolamento nel trattamento dei dati.

Il Responsabile risponde dei danni a lui imputabili se non ha adempiuto agli obblighi a lui specificatamente diretti o ha agito in modo difforme o contrario alle istruzioni del Titolare.

4. SANZIONI

L'art. 82 del GDPR disciplina la responsabilità e il diritto al risarcimento, in forza del quale chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal Titolare del trattamento o dal Responsabile del trattamento.

Il sistema sanzionatorio prevede, a fronte del compimento di violazioni del Regolamento, in funzione delle circostanze di ogni singolo caso, l'applicazione delle seguenti sanzioni amministrative pecuniarie:

- una multa fino a 10 milioni di euro o, se superiore, fino al 2% del volume d'affari globale registrato nell'anno precedente, nei casi previsti dall'articolo 83, paragrafo 4 del Regolamento (a titolo esemplificativo, in caso di: mancata adozione delle tutele per i minori, sui dati anonimizzati, delle misure *privacy by design* e *by default*, contitolari, registri del trattamento, *privacy impact assessment*, istruzioni agli autorizzati, misure di sicurezza, *data protection officer*);
- una multa fino a 20 milioni di euro o, se superiore, fino al 4% del volume d'affari globale registrato nell'anno precedente, nei casi previsti dall'articolo 83, paragrafi 5 e 6 del Regolamento (a titolo esemplificativo, in caso di mancato rispetto dei principi di base del trattamento, dei diritti degli interessati, delle regole sui trasferimenti di dati extra UE, ecc.).

Nell'ambito del GDPR viene stabilito un margine di discrezionalità circa la possibilità di infliggere una sanzione e la determinazione dell'importo della stessa. Ciò non implica un'autonomia gestionale delle sanzioni in capo alle Autorità nazionali competenti, ma fornisce, a queste ultime, alcuni criteri su come interpretare le singole circostanze del caso. I criteri per la determinazione delle sanzioni amministrative pecuniarie (come, a titolo esemplificativo, la natura, gravità e durata della violazione, il carattere doloso o colposo della violazione, il grado di cooperazione con l'Autorità di controllo al fine di porre rimedio alla violazione e attuarne i possibili effetti negativi) sono stabiliti all'articolo 83 paragrafo 2 del Regolamento.

In sede di adeguamento nazionale alle disposizioni del GDPR, il D.lgs. 196/2003, come modificato dal D.lgs. 101/2018, all'art. 166 ha fornito ulteriori indicazioni in relazione ai criteri di applicazione delle sanzioni amministrative pecuniarie e in relazione al procedimento per l'adozione dei provvedimenti correttivi e sanzionatori.

È offerta all'Autorità nazionale l'opportunità di sostituire la sanzione pecuniaria con un ammonimento, "*in caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica*" (cfr. Considerando 148).

Secondo quanto stabilito dal Considerando 149 e dall'art. 84 del GDPR, l'Italia ha introdotto disposizioni relative a sanzioni penali come strumento di attuazione e tutela della nuova disciplina. In particolare, il D.lgs. 196/2003, come modificato dal D.lgs. 101/2018, ha previsto specifiche fattispecie penali agli artt. 167, 167 bis, 167 ter, 168, 170 e 171.

Secondo l'articolo 58 del GDPR, le Autorità possono avvalersi inoltre di una serie di poteri correttivi come la possibilità di limitare o addirittura vietare un trattamento dei dati da parte dell'azienda. Tutto ciò potrebbe portare l'organizzazione ad un'interruzione di un servizio o un'attività aziendale.

5. ESIMENTE DELLA RESPONSABILITÀ

L'adozione di un Modello Organizzativo Privacy (e delle procedure di attuazione) consente ad imprese, enti ed organizzazioni di sottrarsi all'imputazione della responsabilità. Tuttavia, per esimersi dalla responsabilità a suo carico, l'impresa, l'ente o l'organizzazione deve dare la dimostrazione di avere adottato, efficacemente attuato e applicato tutte le misure statuite nell'ambito del MOP in conformità alle previsioni del Regolamento. Al fine di garantire l'efficacia del MOP, il GDPR richiede di implementare un approccio *risk based*, ossia il Titolare deve:

- esaminare (attraverso uno o più "*assessment*") le operazioni di trattamento e individuare e valutare l'esistenza di possibili rischi per la sicurezza e i diritti e le libertà degli interessati ("*valutazione di rischio e impatto*" o anche "*Risk e Privacy Impact Assessment*");
- individuare le attività di *remediation* e *implementation* da compiere, attraverso un programma prioritizzato di adeguamento ed effettiva attuazione delle azioni stesse;
- nel contesto della fase di *remediation*, prevedere specifiche procedure dirette ad attuare e controllare il programma di adeguamento, anche in relazione alla formazione e attuazione delle decisioni che consentono all'impresa, ente o organizzazione di operare in conformità al Regolamento;
- individuare modalità di analisi, valutazione e gestione delle risorse finanziarie necessarie ad attuare il programma di adeguamento;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello Organizzativo Privacy;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello Organizzativo Privacy.

Al fine di garantire l'effettiva applicazione del Modello Organizzativo Privacy deve essere previsto quanto segue:

- una verifica periodica, e, nel caso in cui siano scoperte significative violazioni del Modello Organizzativo Privacy o intervengano mutamenti nell'organizzazione o nelle attività ovvero modifiche legislative, la modifica del Modello Organizzativo Privacy;
- l'irrogazione di sanzioni in caso di violazione delle prescrizioni imposte dal Modello Organizzativo Privacy.

PARTE SPECIALE

6. IL MODELLO ORGANIZZATIVO PRIVACY DI SIPAG BISALTA

6.1 FINALITÀ DEL MODELLO ORGANIZZATIVO PRIVACY

Il presente documento costituisce il Modello Organizzativo Privacy di SIPAG BISALTA (di seguito "**SIPAG**"), che effettua trattamenti di dati personali, nella sua qualità di Titolare e/o di Responsabile.

Tale documento descrive le attività poste in essere da Sipag per assicurare la conformità al GDPR e il relativo approccio metodologico utilizzato, oltre agli aspetti di governance, risk management e compliance applicabili alla protezione dei dati personali con la finalità di definire:

i. i meccanismi organizzativi e gestionali, inclusi ruoli, responsabilità in materia di protezione dei dati personali ("**governance**");

ii. le modalità di gestione dei rischi in materia di protezione dei dati personali ("**risk management**") un sistema strutturato di procedure a presidio dei rischi che sono stati rilevati, nonché una costante azione di monitoraggio sulla corretta attuazione di tale sistema in conformità ai requisiti normativi applicabili in materia di protezione dei dati personali ("**compliance**").

Sipag, consapevole dell'importanza di adottare ed efficacemente attuare un Modello Organizzativo Privacy, ha predisposto questo documento, che costituisce un valido strumento di sensibilizzazione dei destinatari (come definiti al paragrafo 6.2) per dare evidenza delle procedure già operative, con decorrenza dalla entrata in vigore del GDPR e dei comportamenti conformi ai requisiti del GDPR.

6.2 DESTINATARI

Le disposizioni del presente Modello Organizzativo Privacy sono vincolanti per i dipendenti (ivi inclusi i dirigenti) di Sipag, per i collaboratori sottoposti a direzione o vigilanza dei dipendenti di Sipag e per tutti coloro che, pur non appartenendo a Sipag, operano a vario titolo gestendo attività che implicano il trattamento di dati personali (di seguito i "**Destinatari**").

6.3 ELEMENTI FONDAMENTALI DEL MODELLO ORGANIZZATIVO PRIVACY

Gli elementi fondamentali del Modello Organizzativo Privacy, sviluppati nell'ambito delle attività di adeguamento al GDPR, possono essere così riassunti:

- la predisposizione e adozione di una Procedura per la gestione del Data Breach (GDPR 03);
- la redazione di istruzioni per la gestione della documentazione aziendale (GDPR 04, GDPR 07);
- l'aggiornamento della documentazione privacy rilevante (es. informative, consensi, nomine interne ed esterne: GDPR 09, GDPR 09_1, GDPR 09_2, GDPR 09_3, GDPR 09_3.1, GDPR 10_1, GDPR 10_2, GDPR 10_3, GDPR 11.1, GDPR 11.2, GDPR 11.3, GDPR 11.4);
- l'adozione e l'aggiornamento del Registro dei trattamenti (GDPR 01);
- la programmazione di attività di informazione e formazione sui contenuti e i cambiamenti introdotti dal GDPR e volte alla diffusione del presente Modello Organizzativo Privacy (GDPR 05);
- la previsione di implementazione di attività periodiche di verifica, anche a campione, per il monitoraggio sull'adeguata attuazione del GDPR, sull'efficacia ed effettiva operatività del Modello Organizzativo Privacy, anche ai fini del riesame dello stesso, e del sistema delle procedure adottate (Piano Audit).

6.4 RIFERIMENTI NORMATIVI

Il presente documento fa riferimento e si ispira alle seguenti norme:

- "*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*";
- Decreto Legislativo 10 agosto 2018, n. 101 "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*";
- Standard UNI EN ISO / IEC 27001:2013 "*Tecnologia per l'Informazione – Tecniche per la Sicurezza – Sistemi di Gestione per la Sicurezza delle Informazioni – Requisiti*";
- Linee Guida e Provvedimenti specifici dell'Autorità Garante per la Protezione dei Dati Personali;
- ARTICLE 29 DATA PROTECTION WORKING PARTY: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

6.5 TERMINI E DEFINIZIONI

Si riportano le definizioni e gli acronimi utilizzati nel presente documento.

Analisi e Valutazione del rischio: Processo complessivo di comprensione della natura del rischio, determinazione del livello di rischio per la protezione dei dati personali, analisi del rischio e ponderazione del rischio, sia in termini di rischio per la sicurezza dei dati, che di rischio di impatto sulle libertà individuali. Identificazione del rischio Processo di analisi, individuazione e descrizione dei rischi.

Autorizzato, Responsabile (interno): è il soggetto persona fisica che opera alle dipendenze del Titolare, ma anche del Responsabile se nominato, ed effettua, materialmente le operazioni di trattamento sui dati personali. E' definito Responsabile il soggetto che, con riferimento alla quantità di dati e alla criticità degli stessi, è contraddistinto da maggiore responsabilizzazione, anche in ragione della autonomia operativa. L'autorizzato è un mero esecutore di compiti.

Conseguenza: Esito di un evento che influenza gli obiettivi.

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.

Fonte del rischio: Elemento che da solo o in combinazione con altri possiede il potenziale intrinseco di originare il rischio.

GDPR: General Data Protection Regulation (Regolamento Europeo UE 2016/679).

Impatto: Conseguenze dei rischi del trattamento sui diritti e le libertà degli interessati, considerati la natura, l'oggetto, il contesto e le finalità del trattamento (es. a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), nonché le misure tecniche e organizzative implementate per contrastare/mitigare i rischi.

Livello del Rischio: Espressione quantitativa del rischio o combinazione di rischi, espresso in termini di combinazione di conseguenze e della loro verosimiglianza.

Minaccia: Potenziale causa di un incidente indesiderato che può mettere in pericolo un sistema e/o i dati e/o i trattamenti di Sipag.

Ponderazione del rischio: Processo di comparazione dei risultati dell'analisi del rischio con criteri del rischio al fine di determinare se il rischio e la sua espressione quantitativa sia accettabile o tollerabile.

Responsabile (esterno) 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.

Rischio: Rischio per la sicurezza dei dati e per i diritti e le libertà fondamentali dell'interessato, la cui probabilità e gravità viene determinata con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento, in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato. Anche l'effetto dell'incertezza sugli obiettivi.

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 Europea o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione Europea o degli Stati membri.

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, 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.

Vulnerabilità: Debolezza di un bene o di un controllo che può essere sfruttato da una o più minacce.

Criterio di Rischio: Termini di riferimento a fronte dei quali è valutata la significatività del rischio.

Trattamento del rischio: Processo per modificare e minimizzare il rischio. Controllo: Misura tecnica ed organizzativa adeguata che sta modificando il rischio. Rischio residuo: Rischio che rimane dopo il trattamento del rischio.

6.6 PERCORSO METODOLOGICO DI DEFINIZIONE DEL MODELLO ORGANIZZATIVO PRIVACY: VALUTAZIONE DEL CONTESTO E RISK & PRIVACY ASSESSMENT

Con riguardo a tutte le attività di adeguamento al GDPR, Sipag ha adottato un approccio metodologico in linea con i requisiti del GDPR, gli standard e le best practice in materia di protezione di dati personali.

6.6.1 L'ASSESSMENT: I PRINCIPI

A tal proposito, Sipag, al fine di comprendere il proprio contesto (interno, esterno, ecc.), ha effettuato un'analisi delle proprie attività. Nell'ambito di tale analisi, Sipag ha, in primo luogo, svolto una serie di attività di assessment legale/organizzativo e tecnico.

Tale assessment è stato svolto suddividendo l'attività come segue:

i. raccolta delle informazioni utili alla predisposizione del Registro dei trattamenti adottato da Sipag in adempimento agli obblighi di legge;
ii. raccolta della documentazione privacy rilevante;
iii. raccolta delle informazioni sui flussi informativi e sui sistemi a supporto dei trattamenti censiti e valutazione delle misure di sicurezza tecnologiche;
iv. esame dei sistemi e delle misure di sicurezza;
v. valutazione delle misure tecniche e organizzative, del rischio di sicurezza e dei rischi di impatto

del trattamento sui diritti e le libertà individuali degli interessati;

vi. valutazione complessiva del rischio di impatto sui diritti e sulle libertà degli interessati.

La relativa documentazione è disponibile presso la sede legale, che ne cura l'archiviazione, rendendola disponibile per eventuale consultazione a chiunque sia legittimato a prenderne visione.

6.6.2 L'ASSESSMENT: ANALISI E VALUTAZIONE DEL CONTESTO

I dati personali trattati sono influenzati da fattori inerenti il contesto di riferimento esterno ed interno. Tali fattori costituiscono anche la fonte dei rischi per la protezione dei dati personali e sono stati valutati nel contesto degli assessment sopra esposti.

La valutazione del contesto esterno deve prendere in considerazione i seguenti fattori:

- contesto settoriale: valutazione degli aspetti inerenti fornitori, terze parti, visitatori del settore in cui Sipag opera;
- contesto normativo: valutazione dell'applicabilità del GDPR e di normative, incluse specifiche normative di settore, a Sipag in materia di protezione dei dati personali;
- contesto tecnologico: valutazione dell'andamento di minacce e vulnerabilità inerenti l'utilizzo dei sistemi informatici per il trattamento dei dati personali;
- contesto socio-economico: valutazione del valore intrinseco dei dati personali trattati da Sipag e potenziali minacce;
- contesto territoriale: valutazione delle caratteristiche del contesto territoriale esterno ad Sipag e del relativo impatto sulla protezione dei dati personali.

Contesto interno

La valutazione del contesto interno deve prendere in considerazione i seguenti fattori:

- contesto legale: valutazione della natura giuridica e della responsabilità di Sipag;
- contesto organizzativo e delle risorse umane: valutazione del modello organizzativo e delle risorse umane mediante cui è effettuato il trattamento dei dati personali;
- contesto IT: valutazione dei servizi IT, della relativa infrastruttura IT, dei sistemi mediante cui è effettuato il trattamento dei dati personali e relative misure di sicurezza.;
- contesto fisico e ambientale: valutazione dei siti fisici (sedi) e delle caratteristiche ambientali mediante cui è effettuato il trattamento dei dati personali.

6.6.3 L'ASSESSMENT: ANALISI DELLE PARTI COINVOLTE NELLA PROTEZIONE DI DATI PERSONALI

Le principali parti coinvolte nella protezione di dati personali individuate da Sipag nel corso dell'assesment risultano analiticamente descritte e formalizzate nel documento GDPR 09 "*Organigramma – Compiti – Responsabilità*".

6.6.4 L'ASSESSMENT: ANALISI DEL RISCHIO

Con l'introduzione del GDPR la privacy diventa risk based.

Sipag, nell'ambito delle attività di adeguamento al GDPR, ha esaminato e gestito (e intende gestire) il rischio secondo il seguente ciclo di attività:

i. identificazione dell'architettura, delle parti coinvolte dei ruoli e delle responsabilità per la gestione dei rischi;

ii. attuazione della gestione del rischio, attraverso le attività di analisi e valutazione del rischio (*risk assessment*), di trattamento dei rischi - cioè di individuazione, attuazione delle misure

organizzative e tecniche a mitigazione dei rischi, nonché di attribuzione di una priorità alle stesse (*remediation* e *implementation*);

iii. monitoraggio e riesame del modello (*monitoring for continuous improving*) volto a realizzare un miglioramento continuo del sistema di gestione dei rischi di data protection.

La protezione dei dati personali viene effettuata da Sipag nell'ottica del perseguimento dei seguenti obiettivi strategici:

- confidenzialità dei dati personali trattati;
- disponibilità dei dati personali trattati, anche a seguito di incidenti che potrebbero comportare la perdita di continuità operativa nel trattamento di tali dati e dei correlati obiettivi di resilienza;
- integrità dei dati personali trattati.

La mappatura dei trattamenti, unitamente all'analisi delle misure implementate e in corso di costante aggiornamento, nonché la valutazione dei rischi connessi a ciascun trattamento, sono documentate all'interno del Registro delle Attività di trattamento, che illustra anche la metodologia adottata.

6.6.5 L'ASSESSMENT: LA GAP ANALYSIS

A seguito *dell'assesment*, è stata effettuata la relativa *gap analysis* al fine di individuare:

1. eventuali scostamenti rispetto ai requisiti ("***gap analysis***");
2. eventuali piani di riallineamento ("***remediation plan***").

6.6.6 LA REMEDIATION: I PRINCIPI

A seguito dell'ultimo *assesment* effettuato, Sipag ha ritenuto necessario adottare le seguenti misure:

- Informative privacy e consensi: aggiornamento (es. ai dipendenti, ai collaboratori, ai fornitori, ai visitatori, ai clienti, agli organi ed organismi interni di Sipag) e relativi consensi ove necessari, nonché loro conservazione;

- Procedure: previsione dell'adozione di procedure specifiche in ambito privacy, al fine di formalizzare corrette prassi già in vigore;

- Nomine soggetti interni: riformalizzazione delle nomine ad Soggetto Autorizzato o a Responsabile interno del trattamento e ad Amministratore di sistema, con migliore dettaglio di compiti e responsabilità, in modo tale da definire l'ambito di trattamento consentito ai soggetti interni che trattano i dati personali. In tale contesto, sono previsti profili di autorizzazione ai dati diversificati per trattamento posto in essere dagli Incaricati, in modo da limitare l'accesso ai dati ai soli soggetti autorizzati;

- Nomine soggetti esterni: adozione delle nomine di soggetti terzi che accedono ai dati a Responsabile esterno del trattamento e ad Amministratore di sistema. In tale contesto, si prevede di mantenere la lista dei fornitori esterni – ed in particolare di quelli che trattano dati personali – aggiornata periodicamente;

- Amministratori di sistema: aggiornamento delle nomine;

- Modello Organizzativo Privacy: adozione del presente MOP, quale documento di sintesi delle procedure e prassi già in vigore o di nuova adozione;

- Misure di sicurezza: adozione e/o formalizzazione di processi adeguati con riferimento alla sicurezza dei dati personali e adozione o rinforzo delle misure di sicurezza sui sistemi;

- Formazione: formalizzazione in procedura della previsione di formazione periodica (già in precedenza attuata) dei dipendenti e collaboratori in materia di protezione dei dati personali, al fine di fornire le corrette

istruzioni operative (art.29 GDPR): le formali designazioni sono prive di valore in assenza di corrette istruzioni perché nessuno può essere considerato responsabile di una violazione delle procedure se non ha ricevuto le istruzioni in merito alla procedura.

- Registro dei trattamenti: revisione ed aggiornamento registro per tracciare tutti i trattamenti effettuati (a titolo esemplificativo inserimento trattamento per procedura whistleblowing);

- Mantenimento: adozione di processi di verifica periodica della conformità al GDPR.

6.6.7 LA REMEDIATION: LE POLITICHE

- ***Politiche per la protezione dei dati personali***

SIPAG ha ritenuto necessario impegnarsi ad assicurare che tutti i trattamenti di dati personali svolti avvengano nel rispetto dei requisiti cogenti applicabili, con particolare riferimento ai principi e alle regole da osservare.

SIPAG, nell'ambito del presente Modello Organizzativo Privacy e delle procedure adottate e divulgate internamente a SIPAG, formalizza le linee guida in merito ai principi comportamentali e alle nuove regole, pilastri della compliance in materia di protezione dei dati personali, sensibilizzando attraverso adeguate attività di informazione e formazione tutto il personale, compresi coloro che collaborano con SIPAG, in merito alla sistematica e puntuale osservanza degli stessi principi e regole.

In particolare, sono state adottate e/o sono in corso di adozione, ad esempio le seguenti procedure:

- Data Retention che descrive quali dati sono trattati da SIPAG, quali sono i tempi di trattamento necessario e quindi di conservazione;

- Data Breach, che descrive il processo di notifica all'Autorità e all'Interessato, ove ritenuto necessario, delle violazioni di dati personali;

Per maggiori dettagli si rimanda alle procedure GDPR pubblicate nella intranet di SIPAG.

6.6.8 LE INFORMATIVE, I CONSENSI

SIPAG ha ritenuto necessario impegnarsi ad assicurare che tutti i soggetti di cui si trattano dati personali vengano adeguatamente informati. Per questo, SIPAG ha pianificato l'aggiornamento di tutte le informative agli interessati e dei relativi consensi e l'attività di sensibilizzazione per i dipendenti e i collaboratori.

6.6.9 LE NOMINE E LE ISTRUZIONI

SIPAG ha ritenuto necessario impegnarsi ad assicurare che tutti i soggetti che trattano dati personali vengano adeguatamente informati ed istruiti. Per questo, SIPAG ha pianificato la nomina a Responsabili interni ed esterni del trattamento e di Incaricati del trattamento.

6.6.10 LA FORMAZIONE

SIPAG ha ritenuto necessario impegnarsi ad assicurare che tutti i soggetti che trattano dati personali vengano adeguatamente formati.
Per questo, SIPAG ha pianificato una formazione adeguata sia agli Incaricati del trattamento che ai Responsabili interni del trattamento, relativamente ai contenuti del GDPR e alle procedure adottate da SIPAG.

6.6.11 IL REGISTRO DEI TRATTAMENTI

Il Registro dei trattamenti comprende le attività di trattamento svolte sotto la responsabilità del Titolare del trattamento e contiene tutte le informazioni richieste dall'art. 30, paragrafo 1 del Regolamento per la redazione del Registro dei Trattamenti da parte del Titolare;
A tal proposito, per maggiori dettagli si rimanda a quanto evidenziato nell'ambito del Registro dei trattamenti di SIPAG.

6.6.12 I DIRITTI DEGLI INTERESSATI

SIPAG ha ritenuto necessario impegnarsi ad assicurare che gli interessati possano adeguatamente esercitare i propri diritti e che gli Incaricati ne siano a conoscenza. A tal riguardo, sono state predisposte informative adeguate e procedure di gestione dei diritti degli Interessati.

6.6.13 IL SISTEMA DI CONTROLLO INTERNO DI SIPAG

SIPAG ritiene necessario impegnarsi ad assicurare l'adozione di adeguati strumenti di controllo, monitoraggio, audit e riesame della privacy di SIPAG.
A tal fine, SIPAG ha predisposto il presente Modello Organizzativo Privacy, che tiene conto del sistema di controllo interno, finalizzato a verificare l'idoneità o l'efficacia e l'effettiva operatività degli specifici controlli a presidio dei rischi di compliance che sono stati identificati.
Il sistema di controllo coinvolge ogni settore dell'attività svolta da SIPAG attraverso la distinzione dei compiti operativi da quelli di controllo, riducendo ragionevolmente ogni possibile conflitto di interesse.
In particolare, il sistema di controllo interno di SIPAG si basa sia sulle regole comportamentali previste nel presente Modello Organizzativo Privacy sia sui seguenti elementi:

- il Codice Etico;
- Modello 231/01;
- un sistema di procedure interne;
- la struttura gerarchico-funzionale (organigramma), le parti coinvolte nella protezione dei dati personali (anche soggetti interni ed esterni, Responsabili e Incaricati) del trattamento e le strutture organizzative di governo e vigilanza di SIPAG;
- il sistema di deleghe e procure;
- sistemi informativi orientati alla segregazione delle funzioni e alla protezione delle informazioni in essi contenute;
- la tracciabilità delle operazioni, in base alla quale queste devono, nei limiti del possibile, essere adeguatamente documentate e i processi di decisione, autorizzazione e svolgimento delle operazioni devono essere verificabili ex post anche tramite appositi supporti documentali.

7. ORGANI E FUNZIONI COINVOLTI NELLA DATA PROTECTION

7.1 ORGANIGRAMMA PRIVACY

SIPAG ha strutturato il proprio organigramma privacy come da documenti GDPR 09, GDPR 09_1, GDPR 09_2, GDPR 09_3, a cui integralmente si rinvia.

7.2 DESIGNAZIONE DEL DATA PROTECTION OFFICER

Nell'ambito del programma di adeguamento al GDPR dalle verifiche è emersa la non obbligatorietà di designazione della figura del Data Protection Officer (DPO) ai sensi dell'art. 37 del GDPR. La eventuale nomina su base volontaria sarà oggetto in ogni caso di eventuali ulteriori valutazioni.

7.3 LE FUNZIONI DI GOVERNANCE DEL MODELLO ORGANIZZATIVO PRIVACY.

Attesa la non obbligatorietà della nomina del DPO gli aspetti relativi alla *Data Protection,* all'interno di SIPAG, sono curati principalmente dal Referente Privacy, dal Responsabile IT e dal Responsabili HR, insieme alle ulteriori funzioni di volta in volta coinvolte nella valutazione ed analisi di tematiche specifiche in materia di *data protection*.

Le suddette aree aziendali hanno il compito, con il coordinamento del Referente Privacy, di:

- informare e fornire consulenza al Titolare o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR, nonché da altre disposizioni nazionali o dell'Unione Europea relative alla protezione dei dati;
- sorvegliare l'osservanza del GDPR del Titolare o del Responsabile del trattamento in materia di

protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- esprimere valutazioni in merito all'opportunità di coordinare i Responsabili coinvolti nella valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del GDPR;
- gestire le comunicazioni e le segnalazioni all'Autorità Garante per la protezione dei dati personali;
- supportare il Titolare nella tenuta del Registro dei trattamenti, attenendosi alle istruzioni impartite dallo stesso. In particolare, i suddetti Dipartimenti si occupano di monitorare periodicamente l'efficacia e applicazione delle procedure di SIPAG e del Modello Organizzativo Privacy e fornire supporto nell'aggiornamento periodico del Registro dei trattamenti, così come delle procedure e del Modello Organizzativo Privacy ove necessario;
- curare il costante aggiornamento e revisione del framework documentale privacy (es. informative agli interessati, nomine a Responsabili esterni, autorizzazioni al trattamento, nomine agli Amministratori di Sistema, ecc.);
- curare la predisposizione, la manutenzione e l'aggiornamento del Registro delle Attività di trattamento, anche eventualmente mediante l'ausilio di professionisti esterni;
- verificare la predisposizione delle procedure interne di gestione degli adempimenti privacy (es. procedura di gestione del data breach, policy di data retention, istruzioni per la gestione della documentazione);
- curare la pianificazione e l'attuazione di formazione dedicata in materia di privacy al personale autorizzato al trattamento dei dati personali;
- supportare la pianificazione di Audit volti a verificare periodicamente il corretto adempimento degli obblighi di legge in materia di privacy ed il rispetto delle procedure e delle istruzioni da parte del personale autorizzato al trattamento dei dati personali.

7.4 MONITORAGGIO, VALUTAZIONI E MIGLIORAMENTO CONTINUO

SIPAG, in qualità di Titolare, ed i Referenti interni del trattamento devono monitorare in modo sistematico l'adeguatezza, l'efficacia e l'effettiva operatività del Modello Organizzativo Privacy in materia di protezione dei dati personali.

Con riguardo all'adeguatezza, all'efficacia e all'effettiva operatività, la valutazione del Modello Organizzativo Privacy (*assessment*) deve essere effettuata, a titolo esemplificativo e non esaustivo, a fronte di:

- modifiche o evoluzioni del contesto esterno di riferimento, incluse variazioni dei requisiti normativi in materia di protezione di dati personali;
- modifiche o evoluzioni contesto interno di riferimento, incluse evoluzioni che comportano nuovi o mutati trattamenti, finalità di trattamento, scenari di rischio, ecc.;
- modifiche ai sistemi informativi utilizzati per il trattamento dei dati personali;
- esiti degli audit interni che evidenziano non conformità dei trattamenti rispetto ai requisiti applicabili, inclusi i requisiti definiti dallo stesso Titolare del trattamento;
- riesame, su base annuale o comunque periodica; riesame su base occasionale in caso di:
  - gravi o ripetute non conformità, incluse violazioni dei requisiti normativi o dei requisiti definiti dallo stesso Titolare del trattamento;
  - incidenti in materia di protezione dei dati personali (cd. "*Data breach*"); o significative variazioni del contesto di riferimento esterno, incluse variazioni del quadro normativo;
  - significative variazioni del contesto di riferimento interno.

SIPAG inoltre, consapevole dell'importanza di adottare ed attuare efficacemente un Modello Organizzativo

Privacy, idoneo a prevenire i rischi e i danni derivanti dall'attuazione di illeciti trattamenti degli stessi, promuove il riesame e l'adeguamento continuo del MOP da parte delle competenti funzioni coinvolte in funzione delle opportunità di miglioramento rilevate in sede di valutazione dei rischi, di monitoraggio, di audit e di analisi di incidenti e non conformità.

7.5 SEGNALAZIONI

Al fine di promuovere l'osservanza del GDPR, SIPAG invita a segnalare ogni informazione, azione, operazione e, più in generale, qualsiasi attività posta in violazione delle prescrizioni del GDPR stesso, nonché gli specifici incidenti in relazione ai dati personali.

SIPAG vieta atteggiamenti ritorsivi o qualsiasi altra forma di discriminazione o penalizzazione nei confronti del segnalante.

8. OSSERVANZA E DISPOSIZIONI SANZIONATORIE

In caso di violazione delle disposizioni del presente Modello Organizzativo Privacy da parte dei dipendenti o dei collaboratori di SIPAG, quest'ultima applicherà, con coerenza, imparzialità ed uniformità, sanzioni disciplinari proporzionate alle violazioni e, in ogni caso, in conformità alle disposizioni di legge e del Contratto collettivo nazionale applicabile.

L'osservanza delle disposizioni del presente Modello Organizzativo Privacy deve considerarsi parte essenziale delle obbligazioni contrattuali dei dipendenti di SIPAG ai sensi e per gli effetti dell'art. 2104 c.c. e seguenti.

La violazione delle disposizioni del Modello Organizzativo Privacy potrà costituire inadempimento delle obbligazioni del rapporto di lavoro e/o illecito disciplinare, in conformità alle procedure previste dall'art. 7 dello Statuto dei Lavoratori, con ogni conseguenza di legge, anche con riguardo alla conservazione del rapporto di lavoro e all'eventuale risarcimento dei danni. Inoltre, il rispetto dei principi del presente Modello Organizzativo Privacy rappresenta parte essenziale delle obbligazioni contrattuali assunte dai collaboratori.

La violazione del Modello Organizzativo Privacy da parte di terzi potrà costituire inadempimento delle obbligazioni dagli stessi assunte, con ogni conseguenza di legge anche con riguardo alla facoltà di SIPAG di risoluzione del contratto e all'eventuale risarcimento dei danni.

9. DIFFUSIONE DEL MODELLO ORGANIZZATIVO

SIPAG, consapevole dell'importanza che gli aspetti formativi e informativi assumono in una prospettiva di prevenzione, per assicurare che il trattamento dei dati personali avvenga nel rispetto dei requisiti normativi applicabili, definirà un programma di comunicazione e formazione volto a garantire la diffusione delle competenze e conoscenze necessarie per applicare in modo corretto e sistematico le disposizioni in materia di protezione dei dati personali, incluso il presente Modello Organizzativo Privacy.

L'attività di informazione e formazione deve coinvolgere tutti i dipendenti e i collaboratori, nonché tutte le risorse che in futuro saranno inserite nell'organizzazione SIPAG. A tale proposito, le relative attività formative dovranno essere previste e concretamente effettuate sia al momento dell'assunzione, sia in occasione di eventuali mutamenti di mansioni, nonché a seguito di aggiornamenti e/o modifiche del Modello Organizzativo Privacy.

Con riguardo alla diffusione del Modello Organizzativo Privacy, SIPAG si impegna a:

- inviare una comunicazione a tutto il personale avente ad oggetto l'avvenuta adozione del presente Modello Organizzativo Privacy;
- pubblicare il Modello Organizzativo Privacy sulla intranet e/o comunque renderlo noto mediante altre modalità ritenute idonee;

- organizzare attività formative dirette a diffondere la conoscenza e sviluppare la consapevolezza sulla necessità di perseguire i seguenti obiettivi:
    - trattare i dati personali nel rispetto dei principi e dei requisiti definiti dalla normativa applicabile in materia di protezione dei dati personali;
    - trattare i dati personali in modo da minimizzare i relativi rischi, nella consapevolezza delle conseguenze della inosservanza della normativa, delle procedure e dei controlli operativi definiti da SIPAG;
    - riportare in modo tempestivo e sistematico eventuali violazioni o incidenti in materia di protezione dei dati personali.