ISTITUTO ITALIANO
DI TECNOLOGIA

IL MODELLO ORGANIZZATIVO PRIVACY IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

INDICE

- PARTE GENERALE -

SEZIONE PRIMA

1. IL REGOLAMENTO UE 2016/679 (GDPR)

1.1. IL REGOLAMENTO UE 2016/679 (GDPR) E L'ADEGUAMENTO DELLA NORMATIVA NAZIONALE

Il Regolamento UE 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 intende rafforzare e unificare la protezione dei dati personali entro i confini dell'Unione Europea (UE).

Il nuovo 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, introduce 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 di salute o relativi 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 cosidetti "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 può a sua volta nominare Responsabili esterni ed interni del trattamento, che trattano i dati personali per conto del Titolare e anche gli Incaricati 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** 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.

1.2. I PRINCIPI GENERALI E LE NUOVE REGOLE DA OSSERVARE 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 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) che deve essere designato per fornire una consulenza ed assistenza giuridica e tecnica specialistica sulle questioni afferenti alla data protection. 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 incaricato di 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.

1.3. 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 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.

1.4. SANZIONI

L'art. 82 del GDPR disciplina il diritto al risarcimento e responsabilità 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 incaricati, 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.

1.5. ESIMENTE DELLA RESPONSABILITÀ

L'adozione di un Modello Organizzativo Privacy in materia di Protezione dei Dati Personali ("MOP" o "Modello") consente ad imprese, enti ed organizzazioni di potersi sottrarre 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 Modello in conformità alle previsioni del Regolamento.

Al fine di garantire l'efficacia del Modello, 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;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

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

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

1.6. LE LINEE GUIDA IN MATERIA DI VALUTAZIONE DI RISCHIO E DI IMPATTO SULLA PROTEZIONE DEI DATI ("RISK E PRIVACY IMPACT ASSESSMENT")

La valutazione di rischio e di impatto sulla protezione dei dati, prevista dal Regolamento, obbliga i Titolari a svolgere una valutazione di impatto prima di dare inizio al trattamento, che può imporre anche la consultazione dell'Autorità di controllo nel caso in cui le misure tecniche e organizzative individuate per mitigare l'impatto del trattamento non siano ritenute sufficienti, ovvero quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.

A tal proposito, si segnala che sono state emesse le linee guida WP29[1], che definiscono quando una valutazione di impatto sia obbligatoria, chi e come debba condurla (il Titolare, coadiuvato dal Responsabile della protezione dei dati, se designato), in cosa essa consista, precisando la necessità di considerarla come un processo soggetto a revisione continua e non un adempimento una tantum.

[1] 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.

Tali linee guida in materia di valutazione di impatto sulla protezione dei dati consentono al Titolare del trattamento di disporre di indicazioni utili ad effettuare assessment finalizzati a prevenire rischi privacy e realizzare concretamente un fondamentale pilastro stabilito dal Regolamento ossia la protezione dei dati fin dalla fase di progettazione (**Privacy by Design**) di qualsiasi trattamento.

Le linee guida mirano altresì a promuovere la redazione di:

- un elenco comune dell'Unione Europea delle tipologie di trattamento per le quali è obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati;
- un elenco comune dell'Unione Europea delle tipologie di trattamento per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati;
- criteri comuni sulla metodologia per la realizzazione di una valutazione d'impatto sulla protezione dei dati;
- criteri comuni che specifichino quando è necessario consultare l'Autorità di controllo;
- raccomandazioni, ove possibile, basate sull'esperienza acquisita negli Stati membri dell'UE.

- PARTE SPECIALE –

SEZIONE SECONDA

2. IL MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DI DATI PERSONALI DELLA FONDAZIONE ISTITUTO ITALIANO DI TECNOLOGIA

2.1. FINALITÀ DEL MODELLO

Il presente documento costituisce il Modello Organizzativo Privacy in Materia di Protezione dei Dati Personali (di seguito, anche "MOP" o "Modello Organizzativo") della Fondazione Istituto Italiano di Tecnologia (di seguito "IIT"), che effettua trattamenti di dati personali, nella sua qualità di Titolare e/o di Responsabile.

Tale documento descrive le attività poste in essere da IIT 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 e autorità, in materia di protezione dei dati personali ("governance");

ii. le modalità di gestione dei rischi in materia di protezione dei dati personali ("risk management");

iii. 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").

IIT, consapevole dell'importanza di adottare ed efficacemente attuare un Modello Organizzativo in Materia di Protezione dei Dati Personali, ha approvato questo documento, che costituisce un valido strumento di sensibilizzazione dei destinatari (come definiti al paragrafo 2.2) per assumere comportamenti conformi ai requisiti del GDPR.

2.2. DESTINATARI

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

2.3. ELEMENTI FONDAMENTALI DEL MODELLO

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

- l'adozione di una Procedura per la Pseudonimizzazione dei dati personali;
- l'adozione di una Procedura per la gestione del Data Breach;
- l'adozione di una Procedura per la Valutazione preliminare d'impatto sulla protezione dei dati (P.I.A. - Privacy Impact Assessment);
- la formalizzazione di un documento di Approccio metodologico al Privacy Impact Assessment;
- la previsione di specifiche procedure a presidio delle attività ritenute a rischio privacy: es. gestione dei CV, gestione dei CV Tenure Track, Data Retention;

- l'aggiornamento della documentazione privacy rilevante (es. informative, consensi, nomine interne ed esterne);
- l'adozione e l'aggiornamento del Registro dei trattamenti;
- la designazione del Responsabile della protezione dei dati personali o Data Protection Officer (DPO), con attribuzione di specifici compiti per l'efficace attuazione ed effettiva applicazione della compliance ai sensi del GDPR (ad esempio, fornire consulenza day by day sulle questioni afferenti alla data protection, operare risk assessment, ovvero valutare i rischi, fornire pareri su temi IT/Security ai fini dell'applicazione delle soluzioni e delle misure informatiche di sicurezza più adeguate);
- lo svolgimento di attività di informazione e formazione sui contenuti e i cambiamenti introdotti dal GDPR e dal presente Modello;
- la previsione di periodiche attività di verifica, anche a campione, per il monitoraggio sull'adeguata attuazione del GDPR, sull'efficacia ed effettiva operatività del Modello Organizzativo, anche ai fini del riesame dello stesso, e del sistema delle procedure adottate.

2.4. 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, nonche' 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";
- 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.

2.5. TERMINI E DEFINIZIONI

Si riportano le definizioni degli acronimi utilizzati nel presente documento.

TERMINE	DEFINIZIONE
GDPR	General Data Protection Regulation (Regolamento Europeo UE 2016/679).
Dato Personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, 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.
Titolare del	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo

trattamento	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.
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.
Pseudonimizzazione	Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti ad una persona fisica identificata o identificabile.
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.
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.
Definire il contesto	Definizione dei parametri interni ed esterni da tenere in considerazione quando si gestisce il rischio e si definiscono il campo di applicazione e i criteri del rischio per la politica di gestione del rischio.
Contesto esterno	Ambiente esterno nel quale IIT cerca di conseguire i propri obiettivi. [Il contesto esterno può comprendere: l'ambiente culturale, sociale, politico, cogente, finanziario, tecnologico, economico, naturale e competitivo sia internazionale, nazionale, regionale o locale. Key driver e trend aventi impatto sugli obiettivi di IIT; relazioni, percezioni e valori di portatori di interesse esterni].
Contesto interno	Ambiente interno nel quale IIT cerca di perseguire i propri obiettivi. [Il contesto interno può includere: governance, struttura organizzativa, ruoli e responsabilità; politiche, obiettivi e le strategie poste in essere per perseguirli; le capacità, intese in termini di risorse e conoscenze (es. capitali, tempo, persone, processi, sistemi e tecnologie); i sistemi informativi, i flussi informativi e i processi decisionali le relazioni e le percezioni ed i valori dei portatori di interesse interni la cultura di IIT; standard, linee guida e modelli adottati da IIT; forme ed estensioni delle relazioni contrattuali].
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 rischio.
Fonte del rischio	Elemento che da solo o in combinazione con altri possiede il potenziale intrinseco di originare il rischio.
Vulnerabilità	Debolezza di un bene o di un controllo che può essere sfruttato da una o più minacce.
Minaccia	Potenziale causa di un incidente indesiderato che può mettere in pericolo un sistema e/o i dati e/o i trattamenti di IIT.
Conseguenza	Esito di un evento che influenza gli obiettivi.
Livello del Rischio	Espressione quantitativa del rischio o combinazione di rischi, espresso in termini di combinazione di conseguenze e della loro verosimiglianza.

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.
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.

2.6. PERCORSO METODOLOGICO DI DEFINIZIONE DEL MODELLO: VALUTAZIONE DEL CONTESTO E RISK & PRIVACY ASSESSMENT

Con riguardo a tutte le attività di adeguamento al GDPR che sono state svolte, IIT 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.

2.6.1. L'ASSESSMENT: I PRINCIPI

A tal proposito, IIT ha effettuato, al fine di comprendere il proprio contesto (interno, esterno, ecc.), un'approfondita analisi delle proprie attività.

Nell'ambito di tale analisi, IIT ha, in primo luogo, svolto una serie di attività di assessment legale/organizzativo e tecnico.

Tale assessment ha previsto le seguenti fasi principali:

i. raccolta delle informazioni utili all'aggiornamento e arricchimento del censimento e del Registro dei trattamenti adottato da IIT 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.

All'esito dell'assessment svolto è stato formalizzato un report finale, che ha evidenziato il profilo di rischio privacy e le azioni da avviare. Tale attività è stata conclusa a fine gennaio 2018 con la presentazione del suddetto report al Comitato Esecutivo di IIT.

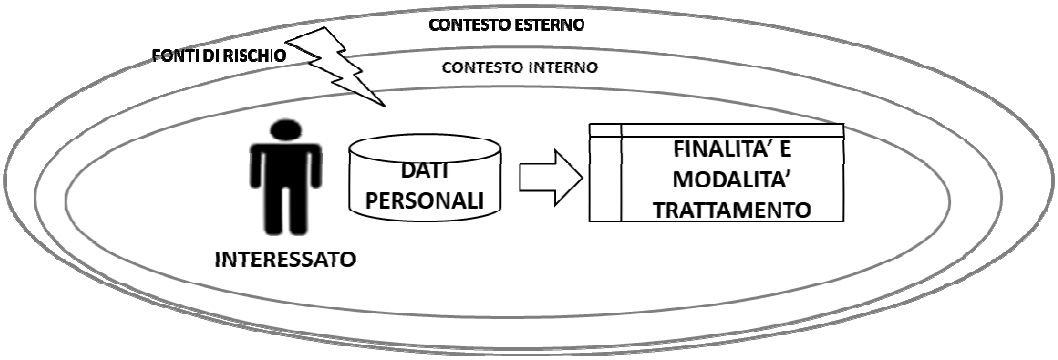
La metodologia adottata è di seguito descritta.

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

2.6.2. 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.

Figura 1 – Valutazione del contesto di riferimento



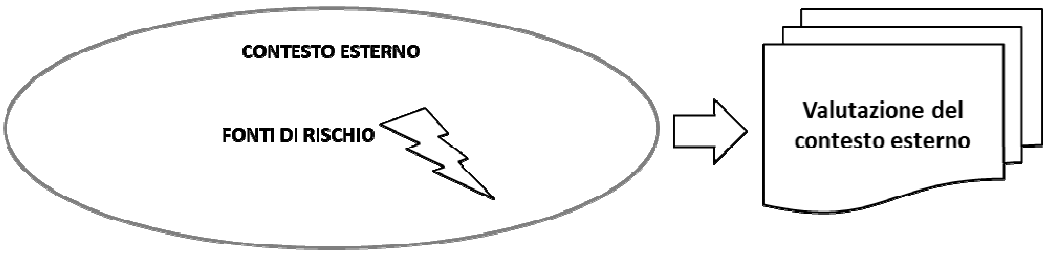
Contesto esterno

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

- contesto settoriale;
- contesto normativo;
- contesto tecnologico;
- contesto socioeconomico;
- contesto territoriale.

TABELLA DEI FATTORI DI VALUTAZIONE DEL CONTESTO ESTERNO	
Contesto settoriale	Valutazione degli aspetti inerenti fornitori, terze parti, visitatori del settore in cui IIT opera.
Contesto normativo	Valutazione dell'applicabilità del GDPR e di normative, incluse specifiche normative di settore, applicabili ad IIT 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 socioeconomico	Valutazione del valore intrinseco dei dati personali trattati da IIT e potenziali minacce.
Contesto territoriale	Valutazione delle caratteristiche del contesto territoriale esterno ad IIT e del relativo impatto sulla protezione dei dati personali.

Figura 2 – Valutazione del contesto esterno



Contesto interno

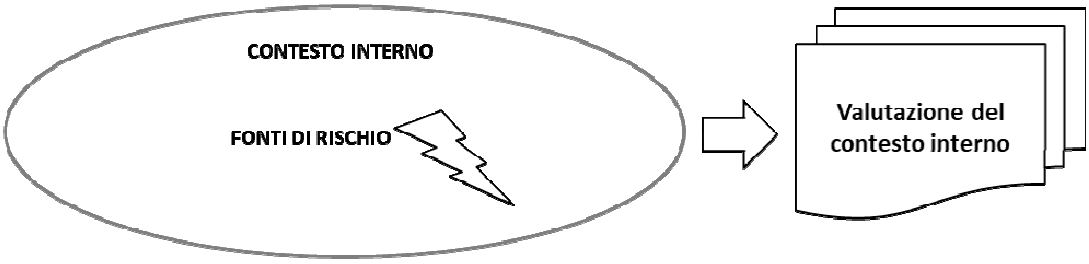
La valutazione del contesto interno deve prendere in considerazione i seguenti fattori:

- contesto legale;

- contesto organizzativo e delle risorse umane;
- contesto IT;
- contesto Fisico e Ambientale.

TABELLA DEI FATTORI DI VALUTAZIONE DEL CONTESTO INTERNO	
Contesto Legale	Valutazione della natura giuridica e della responsabilità di IIT in base a cui è effettuato il trattamento dei dati personali.
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, centrali) e delle caratteristiche ambientali mediante cui è effettuato il trattamento dei dati personali.

Figura 3 – Valutazione del contesto interno



La valutazione del contesto, esterno e interno, di riferimento per la protezione dei dati personali è riportata nei deliverables dell'assessment effettuato.

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

Le principali parti coinvolte nella protezione di dati personali individuate da IIT nel corso dell'assessment sono le seguenti.

TABELLA DELLE PARTI COINVOLTE NELLA PROTEZIONE DEI DATI PERSONALI DI IIT		
PARTE INTERESSATA	COINVOLGIMENTO	ESIGENZE E ASPETTATIVE
Titolare del trattamento	Assicura la conformità ai requisiti della normativa applicabile	Assicurare la conformità ai requisiti applicabili in materia di protezione dei dati personali. Valutare e trattare i rischi in materia di trattamento dei dati. Definire e attribuire ruoli e responsabilità in materia di trattamento dei dati personali internamente alla Società, Titolare del trattamento, e verso soggetti esterni che trattano dati per conto della stessa.
Responsabile esterno del trattamento	Soggetto esterno che tratta dati personali per conto del Titolare	Essere nominato Responsabile esterno del trattamento in conformità ai requisiti del GDPR. Ricevere dal Titolare istruzioni chiare e documentate in merito ai trattamenti da effettuare.
Responsabile interno del trattamento	Soggetto interno che tratta dati personali all'interno di IIT	Essere strumento di accountability e controllo per conto del Titolare. Essere nominato Responsabile interno del

		trattamento in conformità ai requisiti del GDPR. Ricevere istruzioni chiare e documentate in materia di trattamento dei dati personali dal Titolare e fornirle all'Incaricato interno. Ricevere formazione per la corretta applicazione dei requisiti in materia di trattamento dei dati personali. Ricevere sensibilizzazione sui rischi e sulle misure tecnico e organizzative adeguate (c.d. "controlli operativi") in materia di protezione dei dati personali.
Incaricato interno del trattamento	Tratta dati personali all'interno di IIT (es. dipendente, collaboratore)	Ricevere istruzioni chiare e documentate in materia di trattamento dei dati personali dal Titolare e/o dal Responsabile interno. Ricevere formazione per la corretta applicazione dei requisiti in materia di trattamento dei dati personali. Ricevere sensibilizzazione sui rischi e sulle misure tecnico e organizzative adeguate ("controlli operativi") in materia di protezione dei dati personali.
Incaricato esterno del trattamento	Tratta dati personali di IIT ed è incaricato dal Responsabile esterno	Ricevere istruzioni chiare e documentate in materia di trattamento dei dati personali dal Responsabile esterno. Ricevere formazione per la corretta applicazione dei requisiti in materia di trattamento dei dati personali. Ricevere sensibilizzazione sui rischi e sulle misure tecnico e organizzative adeguate ("controlli operativi") in materia di protezione dei dati personali.
Amministratore di sistema	Tratta dati personali all'interno di IIT, essendo incaricato da IIT o dal Responsabile esterno	Ricevere istruzioni chiare e documentate in materia di trattamento dei dati personali dal Titolare. Ricevere formazione per la corretta applicazione dei requisiti in materia di trattamento dei dati personali. Ricevere sensibilizzazione sui rischi e sulle misure tecnico e organizzative adeguate ("controlli operativi") in materia di protezione dei dati personali.
Interessati al trattamento	Soggetto di cui sono trattati i dati personali	Ottenere da IIT, Titolare del trattamento, che i trattamenti dei dati personali siano effettuati nel rispetto dei requisiti applicabili, con particolare rispetto ai principi. Essere informato sui trattamenti effettuati da IIT. Poter esprimere il proprio consenso sui singoli trattamenti, ove necessario. Avere un punto di contatto facilmente utilizzabile per esercitare i propri diritti.
Autorità Garante Privacy	Vigilare sulla corretta applicazione dei requisiti normativi	Ricevere tempestive segnalazioni da parte di IIT, Titolare del trattamento, in caso di incidenti o violazioni in materia di protezione delle informazioni. Ricevere collaborazione da parte di IIT, nell'ambito delle richieste inerenti l'applicazione dei requisiti normativi.

2.6.4. L'ASSESSMENT: ANALISI DEL RISCHIO

- ***Analisi e gestione dei rischi***

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

IIT, nell'ambito delle attività di adeguamento al GDPR, ha esaminato e gestito 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 prioritizzazione delle 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.

Figura 4 – Gestione dei rischi per la protezione dei dati personali

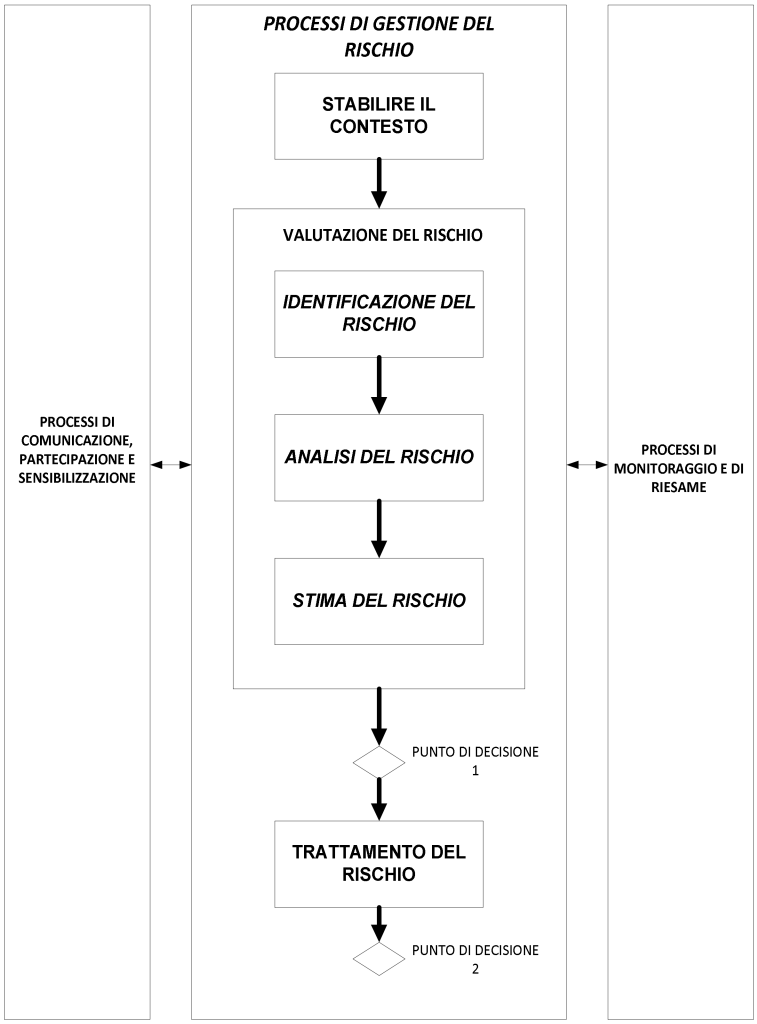


Figura 5 – Valutazione dei rischi e valutazione di impatto

In funzione degli indirizzi adottati, IIT ha deciso di perseguire i seguenti obiettivi strategici in materia di protezione dei dati personali:

1. confidenzialità dei dati personali trattati;
2. 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;
3. integrità dei dati personali trattati.

Figura 6 – Obiettivi per la protezione dei dati personali

Nell'ambito delle attività di adeguamento al GDPR in IIT sono state effettuate le valutazioni delle misure organizzative, delle misure tecniche e del rischio di sicurezza. Tali valutazioni sono state formalizzate nell'ambito del report di fine assessment, e nel Registro dei Trattamenti, a cui si rimanda.

Sulla base del livello di rischio, i criteri di accettabilità del livello di rischio sono definiti come riportato nella seguente tabella.

TABELLA DI STIMA DI ACCETTABILITA' DEL RISCHIO		
CRITERIO	VALUTAZIONE ACCETTABILITA'	OPZIONI
Rischi di livello uguali o superiore a medio basso	Non accettabile	Adottare adeguate misure tecnico organizzative per minimizzarli quanto ragionevolmente possibile
Rischi che implicano la non osservanza di requisiti cogenti	Non accettabile	Adottare adeguate misure tecnico organizzative per minimizzarli quanto ragionevolmente possibile
Rischi che presentano significativi impatti sulle libertà e sui diritti fondamentali degli interessati	Non accettabile	Adottare adeguate misure tecnico organizzative per minimizzarli quanto ragionevolmente possibile

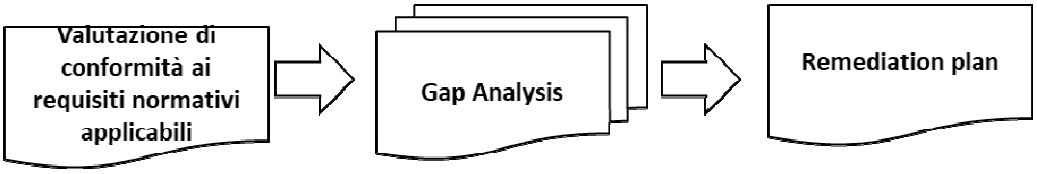
I rischi stimati come non accettabili devono essere oggetto di trattamento mediante la definizione e l'applicazione di misure tecniche e organizzative ("controlli operativi").

2.6.5. L'ASSESSMENT: LA GAP ANALYSIS

A seguito dell'assessment, 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").

Figura 7 – gap analysis e remediation plan



Le azioni di trattamento del rischio, ovvero le misure tecniche e organizzative, identificate in IIT, sono state definite dalla Direzione Affari Legali e dalla Direzione Sistemi Informativi e Telecomunicazioni nel report conclusivo di assessment a cui si rimanda.

2.6.6. LA REMEDIATION: I PRINCIPI

A seguito dell'assessment effettuato, IIT ha ritenuto necessario adottare le seguenti misure adeguate:

- Informative privacy e consensi: aggiornamento e redazione delle informative privacy (es. ai dipendenti, ai collaboratori, ai candidati, ai fornitori, ai visitatori, ai clienti, ai volontari coinvolti nei progetti di ricerca) e relativi consensi;

- Procedure: adozione di procedure specificamente in ambito privacy, quali la procedura relativa alla Pseudonimizzazione dei dati personali, alla gestione del Data Breach, alla Valutazione preliminare d'impatto sulla protezione dei dati (P.I.A. - Privacy Impact Assessment), alla gestione dei CV, alla gestione dei CV Tenure Track, alla Data Retention, ecc.;

- Nomine soggetti interni: adozione delle nomine ad Incaricato del trattamento, a Responsabile interno del trattamento e ad Amministratore di sistema in modo tale da definire l'ambito di trattamento concesso ai soggetti interni che trattano i dati personali. In tale contesto, si prevedono 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 società terze che accedono ai dati a Responsabile esterno del trattamento e ad Amministratore di sistema, prevedendo verifiche periodiche dei fornitori terzi, in particolare sul trattamento dei dati dei dipendenti, in modo tale da avere il controllo sui trattamenti dei dati effettuati per conto di IIT. In tale contesto, si prevede di mantenere la lista dei fornitori esterni – ed in particolare di quelli che trattano dati personali – aggiornata periodicamente;
- Videosorveglianza: redazione e/o aggiornamento delle informative, delle nomine ad Incaricato del trattamento ed a Responsabile del trattamento, del regolamento della videosorveglianza;
- Amministratori di sistema: aggiornamento delle nomine;
- Modello Organizzativo Protezione dei dati personali;
- 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: prevedere la formazione periodica dei dipendenti e collaboratori in materia di protezione dei dati personali;
- Registro dei trattamenti: obbligo di adozione di un registro per tracciare tutti i trattamenti effettuati;
- DPO: obbligo di nominare un DPO che garantisca un miglior controllo della governance dei dati e costituisce una prova dell'accountability del Titolare;
- Mantenimento: adozione di processi di verifica periodica della conformità al GDPR.

2.6.7. LA REMEDIATION: I RUOLI E I COMPITI – GOVERNANCE ED ORGANIZZAZIONE

IIT ha ritenuto quindi misura adeguata individuare i seguenti ruoli e compiti, formalizzati con apposite nomine ed istruzioni:

TABELLA DELLE PARTI COINVOLTE NELLA PROTEZIONE DEI DATI PERSONALI DI IIT		
PARTE INTERESSATA	COINVOLGIMENTO	ESIGENZE E ASPETTATIVE
Titolare del trattamento	Assicura la conformità ai requisiti della normativa applicabile	Assicurare la conformità ai requisiti applicabili in materia di protezione dei dati personali. Valutare e trattare i rischi in materia di trattamento dei dati. Definire e attribuire ruoli e responsabilità in materia di trattamento dei dati personali internamente alla Società, Titolare del trattamento, e verso soggetti esterni che trattano dati per conto della stessa.
Responsabile esterno del trattamento	Soggetto esterno che tratta dati personali per conto del Titolare	Essere nominato Responsabile esterno del trattamento in conformità ai requisiti del GDPR. Ricevere dal Titolare istruzioni chiare e documentate in merito ai trattamenti da effettuare.
Responsabile interno del trattamento	Soggetto interno che tratta dati personali all'interno di IIT	Essere strumento di accountability e controllo per conto del Titolare. Essere nominato Responsabile interno del trattamento in conformità ai requisiti del GDPR. Ricevere istruzioni chiare e documentate in materia di trattamento dei dati personali dal Titolare e fornirle all'Incaricato interno. Ricevere formazione per la corretta applicazione dei requisiti in materia di trattamento dei dati personali. Ricevere sensibilizzazione sui rischi e sulle misure tecnico e organizzative adeguate (c.d. "controlli operativi") in materia di protezione dei dati

		personali.
Incaricato interno del trattamento	Tratta dati personali all'interno di IIT (es. dipendente, collaboratore)	Ricevere istruzioni chiare e documentate in materia di trattamento dei dati personali dal Titolare e/o dal Responsabile interno. Ricevere formazione per la corretta applicazione dei requisiti in materia di trattamento dei dati personali. Ricevere sensibilizzazione sui rischi e sulle misure tecnico e organizzative adeguate ("controlli operativi") in materia di protezione dei dati personali.
Incaricato esterno del trattamento	Tratta dati personali di IIT è incaricato dal Responsabile esterno	Ricevere istruzioni chiare e documentate in materia di trattamento dei dati personali dal Responsabile esterno. Ricevere formazione per la corretta applicazione dei requisiti in materia di trattamento dei dati personali. Ricevere sensibilizzazione sui rischi e sulle misure tecnico e organizzative adeguate ("controlli operativi") in materia di protezione dei dati personali.
Amministratore di sistema	Tratta dati personali all'interno di IIT, essendo incaricato da IIT o dal Responsabile esterno	Ricevere istruzioni chiare e documentate in materia di trattamento dei dati personali dal Titolare. Ricevere formazione per la corretta applicazione dei requisiti in materia di trattamento dei dati personali. Ricevere sensibilizzazione sui rischi e sulle misure tecnico e organizzative adeguate ("controlli operativi") in materia di protezione dei dati personali.
Interessati al trattamento	Soggetto di cui sono trattati i dati personali	Ottenere da IIT, Titolare del trattamento, che i trattamenti dei dati personali siano effettuati nel rispetto dei requisiti applicabili, con particolare rispetto ai principi. Essere informato sui trattamenti effettuati da IIT. Poter esprimere il proprio consenso sui singoli trattamenti, ove necessario. Avere un punto di contatto facilmente utilizzabile per esercitare i propri diritti.
Data Protection Officer (DPO)	Soggetto a cui è affidata la Data Protection di IIT	Fornire consulenza e istruzioni chiare e documentate in materia di trattamento dei dati personali. Fornire formazione per la corretta applicazione dei requisiti in materia di trattamento dei dati personali. Fornire sensibilizzazione sui rischi e sulle misure tecnico e organizzative adeguate ("controlli operativi") in materia di protezione dei dati personali. Tenere i rapporti con l'Autorità Garante. Fungere da punto di contatto per gli interessati e per l'Autorità Garante. Fornire il proprio supporto in tema di Risk e Privacy Impact Assessment e Data Breach notification. Tenere aggiornato il registro dei data breach. Gli ulteriori compiti sono evidenziati alla Sezione 3 di questo Modello.

Direzione Affari Legali	Funzione cui è affidata la gestione della normativa privacy in IIT	Gestire le questioni aventi rilevanza in materia di data protection, fungendo da punto di riferimento interno per le altre Direzioni e/o Uffici e/o Linee di ricerca. Collaborare con il DPO. Tenere aggiornato il registro dei trattamenti, le nomine e le istruzioni agli incaricati, ai responsabili interni/esterni, agli amministratori di sistema, le informative agli interessati. Organizzare la formazione.
Autorità Garante Privacy	Vigilare sulla corretta applicazione dei requisiti normativi	Ricevere tempestive segnalazioni da parte di IIT, Titolare del trattamento, in caso di incidenti o violazioni in materia di protezione delle informazioni. Ricevere collaborazione da parte di IIT, nell'ambito delle richieste inerenti l'applicazione dei requisiti normativi.

2.6.8. LA REMEDIATION: LE POLITICHE

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

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

IIT, nell'ambito del presente Modello e delle procedure adottate e divulgate internamente a IIT, 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 IIT, in merito alla sistematica e puntuale osservanza degli stessi principi e regole.

In particolare, sono state adottate ad esempio le seguenti procedure:

- Valutazione preliminare d'impatto sulla protezione dei dati (P.I.A. - Privacy Impact Assessment), che descrive la metodologia risk based per la valutazione dei trattamenti di dati personali;
- Pseudonimizzazione dei dati personali, che descrive la metodologia con cui effettuare e gestire la pseudonimizzazione dei dati;
- Data Retention che descrive quali dati sono trattati da IIT, quali sono i tempi di trattamento necessario e quindi di conservazione e come deve essere effettuata la relativa cancellazione;
- Gestione di Data Breach, che descrive il processo di notifica al DPO e quindi all'Autorità e all'Interessato, ove ritenuto necessario, delle violazioni di dati personali;
- Gestione dei CV, che fornisce indicazioni sul processo di gestione dei CV dei candidati e dei dipendenti e collaboratori all'interno di IIT;
- Gestione dei CV Tenure Track che fornisce indicazioni sul processo di gestione dei CV dei soggetti coinvolti nel percorso di Tenure Track all'interno di IIT.

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

2.6.9. LA REMEDIATION: LE INFORMATIVE, I CONSENSI

IIT ha ritenuto necessario impegnarsi ad assicurare che tutti i soggetti di cui si trattano dati personali vengano adeguatamente informati.

Per questo, IIT ha pianificato l'aggiornamento di tutte le informative agli interessati e dei relativi consensi, e ha pianificato attività di sensibilizzazione per i dipendenti e i collaboratori. Di ciò è stata data evidenza anche in intranet, oltre che con apposita formazione.

2.6.10. LA REMEDIATION: LE NOMINE E LE ISTRUZIONI

IIT ha ritenuto necessario impegnarsi ad assicurare che tutti i soggetti che trattano dati personali vengano adeguatamente informati ed istruiti.

Per questo, IIT ha pianificato il rilascio di nomine a Responsabili interni ed esterni del trattamento e di istruzioni aggiornate agli Incaricati del trattamento. Di ciò è stata data evidenza con apposita formazione.

2.6.11. LA REMEDIATION: LA FORMAZIONE – LA CONSAPEVOLEZZA

IIT ha ritenuto necessario impegnarsi ad assicurare che tutti i soggetti che trattano dati personali vengano adeguatamente formati.

Per questo, IIT ha pianificato il rilascio di formazione adeguata sia agli Incaricati del trattamento che ai Responsabili interni del trattamento, relativamente ai contenuti del GDPR e alle nuove procedure adottate da IIT.

2.6.12. LA REMEDIATION: IL REGISTRO DEI TRATTAMENTI

A seguito delle attività di assessment condotte, è emerso che IIT tratta dati classificabili come dati personali ai sensi del GDPR.

IIT ha ritenuto necessario aggiornare l'elenco descrittivo di detti trattamenti contenuto nel Registro dei trattamenti.

Il Registro dei trattamenti comprende le attività di trattamento svolte sotto la responsabilità del Titolare/Responsabile del trattamento. La struttura del documento prevede il nome e i dati di contatto del Titolare del trattamento e del Responsabile della protezione dei dati; le finalità del trattamento; la descrizione delle categorie di interessati e di dati personali; le categorie di destinatari dei dati personali; ove applicabile, i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale, l'identificazione del Paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate; ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati..

Di ciò è stata data evidenza anche in intranet, oltre che con apposita formazione.

Figura 8 – Registro dei trattamenti dei dati personali

A tal proposito, per maggiori dettagli si rimanda a quanto evidenziato nell'ambito del Registro dei trattamenti di IIT.

2.6.13. LA REMEDIATION: I DIRITTI DEGLI INTERESSATI

IIT 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 adottate informative adeguate.

2.6.14. LA REMEDIATION: IL SISTEMA DI CONTROLLO INTERNO DI IIT

IIT ha ritenuto necessario impegnarsi ad assicurare l'adozione di adeguati strumenti di controllo, monitoraggio, audit e riesame della privacy di IIT.

A tal fine, ha predisposto il presente Modello Organizzativo in materia di protezione dei dati personali, 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 IIT 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 IIT si basa, oltre che sulle regole comportamentali previste nel presente Modello Organizzativo, anche sui seguenti elementi:

- il Modello di Organizzazione Gestione e Controllo adottato ai sensi del D.lgs. 231 del 2001 ed il Codice di comportamento e di condotta scientifica;
- il sistema di procedure adottate da IIT;
- 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 IIT;
- il sistema di deleghe e procure;
- sistemi informativi integrati e orientati alla segregazione delle funzioni e alla protezione delle informazioni in essi contenute, con riferimento sia ai sistemi gestionali e contabili che ai sistemi utilizzati a supporto delle attività operative di IIT;
- 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;
- il supporto reso, da parte della Direzione Affari Legali alle altre Direzioni e/o Uffici, nella gestione di quelle attività che implichino profili di *compliance* con normative specifiche (es. gestione della protezione dei dati personali);
- le attività periodiche di verifica dell'effettiva operatività dei controlli svolti dalla Direzione Funzioni di Controllo Interno e Gestione Rischi (Internal Audit e Compliance).

L'attuale sistema di controllo interno di IIT, inteso come processo attuato da IIT al fine di gestire e monitorare i principali rischi e consentire una conduzione operativa e organizzativa corretta e sana, è in grado di garantire il raggiungimento dei seguenti obiettivi:

- efficacia ed efficienza nell'impiegare le risorse, nel proteggersi dalle perdite e nel salvaguardare il patrimonio di IIT;
- rispetto delle leggi e dei regolamenti applicabili in tutte le operazioni ed azioni di IIT;
- affidabilità delle informazioni, da intendersi come comunicazioni tempestive ed affidabili a garanzia del corretto svolgimento di ogni processo decisionale.

La responsabilità, in ordine al corretto funzionamento del sistema dei controlli interni, è rimessa a ciascuna Direzione e/o Ufficio e/o Linea di Ricerca per tutti i processi di cui essa sia responsabile (in

proposito, si rimanda alla lett. a) di seguito riportata).

La tipologia di struttura dei controlli esistente in IIT prevede:

a) controlli di linea o di primo livello, svolti dalle singole Direzioni e/o Uffici e/o Linea di Ricerca sui processi di cui hanno la responsabilità gestionale, finalizzati ad assicurare il corretto svolgimento delle operazioni;

b) controlli di secondo livello, trasversali, sui rischi operativi e di non conformità, svolti da strutture apposite quali Compliance, Risk Manager, DPO, ecc.;

c) controlli di terzo livello, volti a valutare il disegno e l'effettiva operatività del sistema di controllo interno, svolti dall'Internal Audit;

Le attività di controllo svolte in tema di Data Protection sono meglio chiarite nelle successive due sezioni del presente Modello Organizzativo.

SEZIONE TERZA

3. ORGANI E FUNZIONI COINVOLTI NELLA DATA PROTECTION

3.1. IL DATA PROTECTION OFFICER

3.1.1. DESIGNAZIONE DEL DATA PROTECTION OFFICER

Nell'ambito del programma di adeguamento al GDPR, IIT ha previsto la designazione del Responsabile della protezione dei dati personali (Data Protection Officer – anche DPO) ai sensi dell'art. 37 del GDPR.

3.1.2. COMPITI DEL DATA PROTECTION OFFICER

Il DPO ha il compito di facilitare l'attuazione del GDPR da parte del Titolare/del Responsabile del trattamento, coopera con l'Autorità e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (artt. 38 e 39 del GDPR).

Il DPO deve poter offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il Titolare del trattamento nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare. Deve inoltre agire in piena indipendenza (Considerando 97 del GDPR) e autonomia, senza ricevere istruzioni e riferendo direttamente ai vertici.

In particolare, il DPO di IIT ha i seguenti compiti:

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

b) 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;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del GDPR;

d) cooperare con il Garante per la protezione dei dati personali;

e) fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

f) supportare il Titolare nella tenuta del Registro dei trattamenti, attenendosi alle istruzioni impartite dallo stesso.

In particolare, il DPO controlla periodicamente l'efficacia e applicazione delle procedure di IIT e del Modello Organizzativo e fornisce supporto nell'aggiornamento periodico del Registro dei trattamenti, così come delle procedure e del Modello Organizzativo ove necessario.

Il DPO riesamina periodicamente anche l'efficacia dei Privacy Impact Assessment effettuati.

Il DPO si occupa anche della notifica dei data breach e dell'aggiornamento del relativo registro.

3.2. DIREZIONE AFFARI LEGALI, DIREZIONE SISTEMI INFORMATIVI E TELECOMUNICAZIONI E LE ALTRE FUNZIONI A SUPPORTO

Al fine di poter espletare i propri compiti, il DPO collabora con la Direzione Affari Legali, con la Direzione Sistemi Informativi e Telecomunicazioni e con le ulteriori funzioni di volta in volta coinvolte nella valutazione ed analisi di tematiche specifiche in materia di data protection (es. HROD, Linee di Ricerca).

3.3. FLUSSI INFORMATIVI NEI CONFRONTI DEL DATA PROTECTION OFFICER

Al fine di poter espletare i propri compiti, il DPO deve essere coinvolto, prima possibile, nelle attività di definizione di misure di mitigazione o prioritizzazione, e in ogni questione relativa al trattamento dei dati personali, ai fini della conformità ai requisiti del Regolamento.

A tal proposito, i Responsabili di Direzioni e/o Uffici e/o Linee di ricerca coinvolti nella gestione dei trattamenti di dati personali devono svolgere le dovute attività di comunicazione e consultazione del DPO secondo quanto previsto dalle specifiche procedure di cui al paragrafo n. 2.6.8.

3.4. MONITORAGGIO, VALUTAZIONI E MIGLIORAMENTO CONTINUO

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

Con riguardo all'adeguatezza, all'efficacia e all'effettiva operatività, la valutazione del Modello Organizzativo (*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 periodica, laddove definito. In caso di riesame, su base occasionale, per:
    - 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");
    - significative variazioni del contesto di riferimento esterno, incluse variazioni del quadro normativo;
    - significative variazioni del contesto di riferimento interno.

IIT inoltre, consapevole dell'importanza di adottare ed attuare efficacemente un Modello Organizzativo in materia di protezione di dati personali ai sensi del GDPR, idoneo a prevenire i rischi e i danni derivanti dall'attuazione di illeciti trattamenti degli stessi, promuove il riesame e l'adeguamento continuo del Modello Organizzativo 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.

3.5. AUTORI DEL MONITORAGGIO, VALUTAZIONI E MIGLIORAMENTO CONTINUO

Il monitoraggio è effettuato, nell'ambito delle proprie funzioni, dal Data Protection Officer.

3.6. SEGNALAZIONI

Al fine di promuovere l'osservanza del GDPR, IIT 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.

A tal fine è stato istituito un canale dedicato di comunicazione per la consultazione diretta del DPO (i.e. indirizzo di posta elettronica dpo@iit.it).

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

Tutte le informazioni e la documentazione relative alle segnalazioni di cui al presente paragrafo sono raccolte e custodite dal DPO.

SEZIONE QUARTA

4. OSSERVANZA E DISPOSIZIONI SANZIONATORIE

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

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

La violazione delle disposizioni del Modello Organizzativo 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 rappresenta parte essenziale delle obbligazioni contrattuali assunte dai collaboratori.

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

5. DIFFUSIONE DEL MODELLO ORGANIZZATIVO

IIT, 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, ha definito 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.

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 IIT. 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.

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

- inviare una comunicazione a tutto il personale avente ad oggetto l'avvenuta adozione del presente Modello;
- pubblicare il Modello sulla intranet e/o su qualsiasi altro strumento di comunicazione ritenuto idoneo;
- 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 IIT;
    - riportare in modo tempestivo e sistematico eventuali violazioni o incidenti in materia di protezione dei dati personali.

La documentazione relativa alle attività di informazione e formazione sarà conservata a cura della Direzione Affari Legali disponibile per la relativa consultazione di chiunque sia legittimato a prenderne visione.