Ministero dell'Università e della Ricerca

Segretariato Generale

MODELLO ORGANIZZATIVO PRIVACY "MOP"

(Ruoli e sistema di responsabilità, ai sensi del Regolamento UE 2016/679)

Ministero dell'Università e della Ricerca

Segretariato Generale

SOMMARIO

Ministero dell'Università e della Ricerca

Segretariato Generale

1 PREMESSA METODOLOGICA

1.1 SCOPO

Il presente documento si propone di definire e descrivere il **Modello Organizzativo Privacy (MOP)** utilizzato per la tutela dei Dati Personali raccolti e trattati dal Ministero, allo scopo di:

- ⇨ definire e implementare una modello operativo in grado di tutelare i Dati Personali durante il loro intero ciclo di vita;
- ⇨ consentire al MUR di verificare l'adempimento degli obblighi derivanti dalla normativa a tutela delle persone fisiche rispetto al trattamento dei dati personali che li riguardano;
- ⇨ aumentare il livello di conoscenza delle tematiche di tutela dei Dati Personali, anche al fine di mitigare i rischi (operativi, reputazionali e di adempimento degli obblighi) relativi ad una loro gestione non corretta;
- ⇨ fornire indicazioni chiare e complete per assicurare la conformità normativa nelle attività di trattamento dei Dati Personali;
- ⇨ individuare in maniera univoca le responsabilità per l'adempimento degli obblighi nei processi trasversali che comportano il coinvolgimento di diversi uffici e assicurare il rapporto con i responsabili, ai sensi dell'articolo 28 del RGPD, e con i contitolari ai sensi dell'articolo 26 del RGPD. Pertanto, nel documento vengono richiamati i principali aspetti organizzativi e gli obblighi per assicurare e dimostrare la conformità dei trattamenti alla normativa in materia ferme restando le disposizioni dell'Unione europea e nazionali applicabili, le direttive del Ministro e gli atti di coordinamento del Segretario Generale, ed in particolare:
  - i ruoli e le responsabilità dei soggetti coinvolti ai vari livelli gestionali, di controllo e operativi, nel trattamento dei Dati Personali nella titolarità del Ministero, in tutte le fasi del processo, dalla raccolta ed elaborazione dei dati sino alla loro dismissione (cancellazione e/o anonimizzazione);
  - le modalità di gestione dei Dati Personali, definendo le relative procedure gestionali e gli strumenti per il monitoraggio e controllo del sistema in materia di "Privacy Compliance".

1.2 CAMPO DI APPLICAZIONE

Il MUR, nell'esercizio delle funzioni e dei compiti spettanti allo Stato in materia di istruzione universitaria, di ricerca scientifica, tecnologica e artistica e di alta formazione artistica musicale e coreutica, nelle aree funzionali individuate dall'articolo 51-ter del decreto legislativo 30 luglio 1999, n.300, è chiamato a gestire:

- ⇨ diverse tipologie di Dati Personali (Comuni, Identificativi, Particolari, Giudiziari, ecc.);
- ⇨ diverse categorie di interessati rispetto ai quali assume il ruolo di Titolare del Trattamento (dipendenti, studenti, docenti, ricercatori, collaboratori esterni, persone fisiche ai fini della gestione dei rapporti contrattuali, convenzionali e di collaborazione, visitatori del sito web del MUR) ovvero Responsabile (ove previsto).

Il presente documento trova applicazione nei confronti di tutti coloro che, indipendentemente dalla tipologia del rapporto di collaborazione (dipendente, collaboratore a progetto, consulente, stagisti), siano autorizzati al Trattamento su Dati Personali nella titolarità del MUR.

2 PRINCIPI GENERALI

2.1 CRITERI ED INDIRIZZI

Per raggiungere gli obiettivi sopra definiti, il MUR adotta misure organizzative per essere in grado di dimostrare in ogni momento il rispetto delle norme in materia e, in particolare dei seguenti principi fondamentali indicati dall'Art. 5 del RGPD (Regolamento generale 2016/679/UE)**:**

1. **liceità, correttezza e trasparenza** - i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
2. **limitazione della finalità** - raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali;
3. **minimizzazione dei dati** - adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
4. **esattezza** - esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
5. **limitazione della conservazione** - conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato;
6. **integrità e riservatezza** - trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

L'osservanza di tali principi è assicurata dai direttori che svolgono le funzioni di titolare, per competenza, con l'adozione di misure tecniche e organizzative adeguate atte a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente alla normativa sin dalla progettazione e con misure di protezione per impostazione predefinita (artt. 24,25 e 26 RGPD) nonché per gestire in maniera trasparente il rapporto con gli interessati mettendoli in condizione di esercitare i propri diritti in maniera rapida ed efficace.

2.2 SISTEMA SANZIONATORIO

La violazione della normativa in materia di protezione dei Dati Personali può esporre il Titolare, il Referente e/o gli Autorizzati/Incaricati a diverse tipologie di responsabilità e conseguenti sanzioni (di carattere amministrativo e/o penale), in base alle norme concretamente violate, ed avere impatti reputazionali negativi.

3 QUADRO NORMATIVO DI RIFERIMENTO

3.1 PRINCIPALI RIFERIMENTI (EUROPEI E NAZIONALI) SULLA PROTEZIONE DEI DATI PERSONALI

- ⇨ Regolamento dell'Unione europea relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento Generale sulla Protezione dei Dati) 2016/679/UE), di seguito "RGPD";
- ⇨ Decreto Legislativo 30 giugno 2003, n.196 "Codice in materia di protezione dei dati personali", così come modificato dal Decreto Legislativo n. 101 del 10 agosto 2018;
- ⇨ Decreto legislativo 10 agosto 2018, n.101
- ⇨ Regole deontologiche di cui all'allegato A al decreto legislativo 30 giugno 2003, n.196;
- ⇨ Prescrizioni relative al trattamento di categorie particolari di dati, in particolare:
    1. Prescrizioni relative al trattamento di categorie particolari di dati nei rapporti di lavoro (aut. gen. n. 1/2016);
    2. Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. n. 9/2016).
- ⇨ Opinion 2/2017 on data processing at work", documento adottato dal Gruppo Art. 29 (avallato dall'EDPB):
- ⇨ "Linee guida in materia di valutazione d'impatto sulla protezione dei dati" - WP 248 del 4/2017;
- ⇨ Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, adottate dall'EDPB il 29 gennaio 2020;
- ⇨ Provvedimento Generale del Garante per la protezione dei dati personali dell'8 aprile 2010 in tema di "Videosorveglianza" e "FAQ in tema di videosorveglianza e protezione dei dati personali", pubblicate a dicembre 2020;
- ⇨ Garante per la protezione dei dati personali- Provvedimento Generale del 10 giugno 2021, Linee guida cookie e altri strumenti di tracciamento;
- ⇨ Garante per la protezione dei dati personali - Provvedimento Generale del 1° marzo 2007, "Linee Guida del Garante per posta elettronica e internet";
- ⇨ Garante per la protezione dei dati personali- Provvedimento Generale del 23 novembre 2006, "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati";
- ⇨ Garante per la protezione dei dati personali- Provvedimento Generale del 27 novembre 2008, "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e successive modifiche ed integrazioni;

- ⇨ Provvedimento del Garante per la protezione dei dati personali del 11 ottobre 2018 sulla Valutazione di Impatto o DPIA.

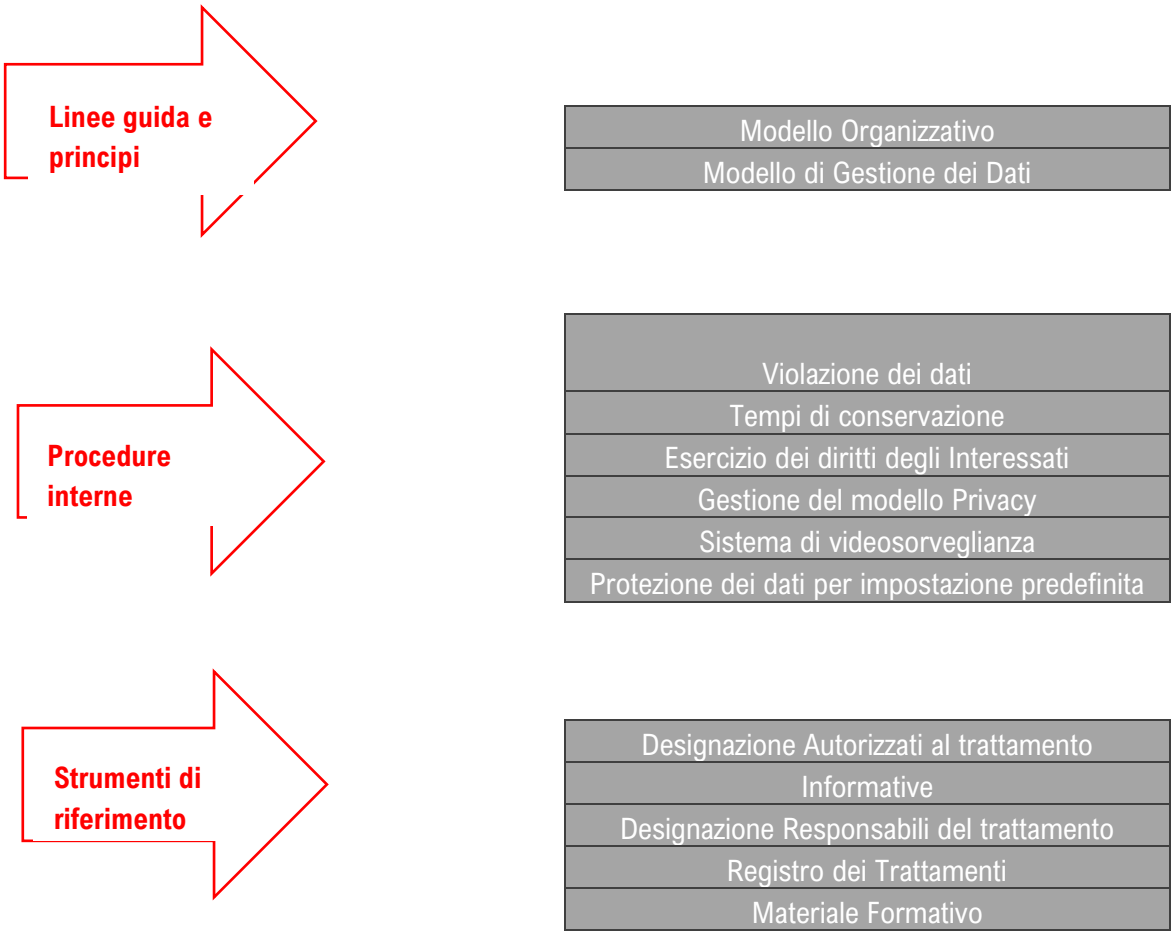
I riferimenti principali, sopra elencati, sono a titolo esemplificativo e non esaustivo e, pertanto, per un quadro aggiornato, direttori, dirigenti e soggetti autorizzati al trattamento possono consultare periodicamente il sito istituzione dell'Autorità garante per la protezione dei dati personali al seguente indirizzo: www.garanteprivacy.it (sezione normativa e provvedimenti)

3.2 RIFERIMENTI NORMATIVI SU ORGANIZZAZIONE ED ATTIVITÀ DEL MUR

- ⇨ Decreto del Presidente del Consiglio dei Ministri 30 settembre 2020, n. 164, rubricato "Regolamento concernente l'organizzazione del Ministero dell'università e della ricerca".
- ⇨ Decreto del Presidente del Consiglio dei Ministri 30 settembre 2020, n. 165, rubricato "Regolamento concernente l'organizzazione degli Uffici di diretta collaborazione del Ministro dell'università e della ricerca.
- ⇨ Decreto del Ministro dell'università e della ricerca e del Ministro dell'economia e delle Finanze n. 1137 dell'1.10.2021, di costituzione dell'Unità di missione di livello dirigenziale generale per l'attuazione degli interventi del Piano Nazionale di Ripresa e Resilienza (di seguito PNRR) a titolarità del Ministero stesso.
- ⇨ Decreto del Ministro dell'università e della ricerca n. 932 del 1° agosto 2022, n. 932 di attivazione della Struttura tecnica di missione di livello dirigenziale generale finalizzata a supportare le attività degli Osservatori, nazionale e regionali, per la formazione sanitaria specialistica, nonché le attività dell'Osservatorio nazionale per le professioni sanitarie
- ⇨ Decreto del Ministro dell'università e della ricerca n. 1100 del 23 settembre 2022, n. 1100 relativo all'attivazione delle struttura tecnica di missione di livello dirigenziale generale, denominata "Struttura tecnica di valutazione dei progetti di ricerca";
- ⇨ Direttiva del Ministro dell'Università e della Ricerca n. 1 dell'8 Gennaio 2021

3.3 FRAMEWORK DI GOVERNO E GESTIONE DEI DATI PERSONALI DEL MUR

Il Framework di Governo e Gestione dei Dati Personali (anche solo Framework) definito dal Ministero è articolato nei seguenti livelli:



- ⇨ **Modello Organizzativo e Gestione dei Dati Personali**, contenuto nel presente documento: definisce le Linee Guida e i Principi Fondamentali di organizzazione e di gestione volti a un corretto governo dei trattamenti dei Dati Personali all'interno del Ministero, in linea con gli adempimenti richiesti dalla normativa vigente.
- ⇨ **Procedure interne**: definiscono regole, attività e relativi ruoli e responsabilità per la gestione di processi per la gestione dei dati personali;
- ⇨ **Strumenti**: rappresentano gli strumenti documentali di riferimento per la gestione e l'aggiornamento degli adempimenti per la protezione dei dati (es. modelli di informative e consenso, nomine, accordi contrattuali con le terze parti), documentazione a supporto della protezione dati (Registro dei trattamenti, procedure per la gestione delle violazioni) e materiale formativo.

3.4 ORGANIGRAMMA FUNZIONALE

Il seguente organigramma riporta le strutture funzionali del MUR (per ulteriori dettagli si rimanda a quanto pubblicato sul sito nella sezione "Organizzazione"):

- ⇨ Segretariato Generale;
- ⇨ Direzione Generale delle istituzioni della formazione superiore;
- ⇨ Direzione Generale degli ordinamenti della formazione superiore e del diritto allo studio;
- ⇨ Direzione Generale della ricerca;
- ⇨ Direzione Generale dell'internalizzazione e della comunicazione;
- ⇨ Direzione Generale del personale del bilancio e dei servizi strumentali;
- ⇨ Unità di missione per il PNRR;
- ⇨ Struttura tecnica di missione per le professioni sanitarie
- ⇨ Struttura tecnica di missione per la valutazione dei progetti di ricerca;

Inoltre, gli Uffici di diretta collaborazione con il Ministro sono i seguenti:

- ⇨ Ufficio di Gabinetto;
- ⇨ Organismo Indipendente di Valutazione della performance del MUR.

3.5 RUOLI E RESPONSABILITÀ IN AMBITO PRIVACY

All'interno dell'Organigramma del MUR, sono identificati i ruoli richiesti dalla normativa privacy:

- ⇨ Titolare / Contitolare del Trattamento (ove previsto);
- ⇨ Responsabile della Protezione dei Dati personali (RPD):
- ⇨ Responsabile del Trattamento;
- ⇨ Amministratore di Sistema.
- ⇨ Autorizzato/Incaricato del Trattamento.

3.5.1 Titolare/contitolare del trattamento dei dati personali

Il Titolare del Trattamento definisce e stabilisce, singolarmente o insieme ad altri (Contitolare), le finalità e le modalità del trattamento dei dati personali. Nell'ambito del Ministero le funzioni di Titolare sono svolte, per competenza, dalle diverse articolazioni interne sulla base dei regolamenti e degli atti di indirizzo strategico del Ministro. Con la Direttiva del Ministro del 8.01.2021 sono stati individuati, in coerenza con le competenze attribuite dai regolamenti interni, i soggetti che esercitano le funzioni di Titolare del trattamento, per i rispettivi ambiti di competenza:

a) il Capo di Gabinetto;
b) il Segretario Generale (con funzioni di coordinamento);
c) i Direttori Generali;
d) il Presidente dell'organismo indipendente di valutazione della performance del MUR

Nel seguito tali soggetti verranno indicati, sinteticamente, come "Esercenti le funzioni di Titolare" del MUR come meglio descritti al punto 4.3.1.

Il Segretario generale nelle sue funzioni di coordinamento ai sensi dell'articolo 5 della Direttiva del Ministro può Delegare alcuni obblighi specifici per trattamenti trasversali che coinvolgono diverse unità organizzative ai Direttori generali

Funzioni, compiti e responsabilità del Titolare del Trattamento:

- ⇨ definire le linee di indirizzo generali del trattamento;
- ⇨ nominare i Responsabili Esterni del Trattamento di Dati Personali;
- ⇨ nominare il RPD;
- ⇨ definire le tipologie di dati personali da raccogliere;
- ⇨ identificare le modalità e i sistemi utilizzati per la raccolta dei dati personali;
- ⇨ definire le finalità della raccolta e del trattamento dei dati personali;
- ⇨ decidere in merito le modalità di trasferimento di dati personali verso Terze Parti;
- ⇨ identificare i termini di conservazione dei dati personali;
- ⇨ attuare le misure per dimostrare, ove necessario, che l'interessato abbia prestato il consenso per il Trattamento dei suoi dati personali;
- ⇨ adottare le misure organizzative e tecniche in ambito privacy adeguate a garantire trattamenti dei dati personali conformi al RGPD (es. adozione dei principi di Data Protection by Design e by Default), come descritto nell'ambito dei paragrafi "Protezione dei dati dall'inizio del trattamento e per impostazione predefinita - Valutazione d'Impatto dei dati (VIA)" e "Sicurezza" collocato all'interno della sezione "Trattamento".

3.5.2 Responsabile della Protezione dei Dati (RPD)

Il Responsabile della Protezione dei Dati Personali è un soggetto designato dal Titolare, o dal Responsabile del trattamento, per assolvere a funzioni di controllo, di consulenza sugli obblighi, formative e informative relativamente all'applicazione del RGPD (ove previsto) e della normativa nazionale in materia di trattamento dei dati personali. Coopera con l'Autorità (e proprio per questo, il suo nominativo va notificato al Garante) e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali.

Funzioni, compiti e responsabilità del RPD indicati dagli articoli 38 e 39 del RGPD sono:

- ⇨ informare e fornire consulenza al Titolare/Responsabile Interno del Trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi previsti dalla normativa in materia;
- ⇨ sorvegliare l'osservanza dei requisiti previsti dal RGPD e dalle altre normative in materia di protezione dei Dati Personali;

- ⇨ fornire un parere nell'ambito della valutazione d'impatto sulla protezione dei Dati Personali (ove applicabile) e sorvegliarne lo svolgimento;
- ⇨ cooperare e fungere da contatto per l'Autorità di protezione dei dati personali per le questioni riferite ai trattamenti;
- ⇨ fungere da punto di contatto tra l'Autorità Garante per la protezione dei dati personali ed il Ministero;
- ⇨ fungere da punto di contatto per gli Interessati e garantire, in cooperazione con gli Esercenti le funzioni di Titolare, la gestione delle richieste di informazione o l'esercizio dei diritti riconosciuti dal RGPD.

3.5.3 Responsabile/Sub Responsabile del Trattamento

Ogni Direttore Esercente le funzioni di Titolare del MUR deve manutenere l'elenco dei Responsabili del trattamento , facenti capo alla propria Direzione, nel Registro dei trattamenti. Il Responsabile del trattamento ai sensi del RGPD è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, esterno rispetto al MUR, che tratta dati personali per conto del MUR Titolare del trattamento.

Il Responsabile del trattamento è vincolato da un contratto o da una convenzione stipulato dall'Esercente le funzioni di Titolare in base alla sopra citata Direttiva dell'8.01.2021.

Le funzioni, compiti e responsabilità del Responsabile del trattamento, sono precisate negli articoli 28 del RGPD, e nel contratto o convenzione stipulata prima dell'inizio dei trattamenti e devono sempre comprendere i seguenti compiti:

- ⇨ effettuare le operazioni di trattamento dei dati personali messi a disposizione dal Titolare nel pieno rispetto dei principi e delle disposizioni della vigente Normativa in materia di protezione dei dati personali ed esclusivamente ai fini dell'esecuzione del Contratto, secondo le modalità, procedure e modulistiche nel tempo indicate dal Titolare;
- ⇨ trattare i dati personali soltanto sulla base delle documentate istruzioni fornite dal Titolare, anche in caso di eventuale trasferimento di dati personali verso soggetti stabiliti in Paesi al di fuori dell'UE, che potrà essere effettuato solo previa autorizzazione del Titolare medesimo e sulla base delle relative istruzioni, adottando le adeguate garanzie secondo la vigente normativa europea e nazionale di riferimento, garanzie di cui andrà mantenuta adeguata documentazione da fornire, ove richiesto, al Titolare;
- ⇨ tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche interessate, adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi identificati;
- ⇨ curare la predisposizione ed il rispetto delle misure prescritte dall'Autorità Garante per la Protezione dei Dati Personali (in seguito il "Garante"), con il provvedimento del 27 novembre 2008, in merito all'attribuzione delle funzioni di "amministratore di sistema" ed, in particolare, procedere a: (i) conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte all'interno della Società quali amministratori del/i sistema/i e, (ii) in tal caso, porre in essere le attività di verifica periodica, con cadenza almeno annuale, sul loro operato, secondo quanto prescritto dal Garante, fino alla eventuale

modifica, sostituzione o abrogazione del provvedimento sopra citato, e (iii) rendere disponibile periodicamente e, in ogni caso, almeno annualmente, la lista aggiornata degli amministratori di sistema;

- ⇨ prestare nei confronti del Titolare la massima collaborazione necessaria a garantire il rispetto, per quanto di relativa competenza, degli obblighi in tema di violazione dei dati personali, di relativa notifica al Garante e, se del caso, di comunicazione agli interessati;
- ⇨ fermo l'obbligo di notificare senza ingiustificato ritardo al Titolare ogni possibile evento qualificabile come violazione dei dati ai sensi dell'articolo 4 n.,12 del RGPD, informare prontamente il Titolare riguardo a qualsiasi ulteriore evento, fatto o circostanza, prevedibile o meno (I.e. incidente di sicurezza), dal quale possa derivare un rischio elevato per i diritti e le libertà fondamentali dei dati personali degli interessati coinvolti nelle operazioni di trattamento;
- ⇨ collaborare con il Titolare nell'assolvimento dell'obbligo di eseguire, in tutti i casi in cui ciò sia necessario, idonea valutazione di impatto sulla protezione dei dati, oltre che ai fini dello svolgimento delle procedure di consultazione preventiva con il Garante o le altre autorità competenti, quando richiesto;
- ⇨ individuare le persone autorizzate al trattamento dei dati personali che operano sotto la propria autorità (in seguito gli "Autorizzati al Trattamento/Incaricati") ed adottare le misure necessarie a (i) garantire l'assunzione da parte di questi ultimi di idonei obblighi di riservatezza in ordine ai dati personali trattati, (ii) fornire loro per iscritto adeguate istruzioni circa il rispetto, in particolare, delle misure per la sicurezza dei dati e (iii) vigilare sulla osservanza, da parte degli Autorizzati al Trattamento/Incaricati, delle istruzioni impartite e, più in generale, delle ulteriori vigenti disposizioni di legge, (iv) controllare e riesaminare, almeno annualmente, i privilegi di accesso ai dati da parte degli Autorizzati al Trattamento/Incaricati (fermo restando la tempestività richiesta dalla cessazione di eventuali rapporti di dipendenza e/o collaborazione);
- ⇨ assicurare il costante monitoraggio degli adempimenti e delle attività effettuate da chi opera sotto la propria autorità;
- ⇨ informare periodicamente il Titolare, su richiesta di quest'ultimo, in ordine all'attività svolta, sia sotto il profilo del trattamento, sia sotto il profilo della sicurezza dei dati;
- ⇨ conservare i dati in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti e successivamente trattati;
- ⇨ inviare al Titolare, previa apposita richiesta scritta, al momento della cessazione delle operazioni di trattamento o anche antecedentemente in caso di specifica richiesta del Titolare, la documentazione comprovante l'avvenuta implementazione degli adempimenti privacy;
- ⇨ informare prontamente il Titolare di ogni questione rilevante in relazione al ruolo di Responsabile del trattamento, quali a titolo indicativo: (i) istanze di interessati; (ii) richieste del Garante; (iii) violazioni o messa in pericolo della riservatezza, della completezza o dell'integrità dei dati personali;
- ⇨ adottare misure tecniche ed organizzative idonee a poter assistere il Titolare nell'assolvimento del proprio obbligo di fornire adeguato riscontro alle richieste di esercizio dei diritti avanzate da parte degli interessati.
- ⇨ comunicare al Titolare qualsiasi richiesta di esercizio di diritti che il Responsabile dovesse ricevere da parte degli interessati, entro un termine massimo di 24 ore dal ricevimento della stessa;

- ⇨ non comunicare a terzi e, più in generale, non diffondere i dati ricevuti, se non in presenza di espressa autorizzazione da parte del Titolare e di adeguati presupposti di liceità per tali ulteriori trattamenti;
- ⇨ prestare nei confronti del Titolare ogni necessaria collaborazione nell'assolvimento di richieste che dovessero pervenire dal Garante o da altre autorità competenti, o in relazione a procedure o ispezioni che dovessero essere avviate nei confronti del Titolare, nonché in caso di controversie avente ad oggetto la normativa a tutela dei dati personali, dando immediata esecuzione alle istruzioni ricevute e fornendo copia di ogni documento richiesto;
- ⇨ consentire l'esecuzione di ogni altra operazione richiesta o necessaria per ottemperare agli obblighi derivanti dalla normativa in materia di protezione dei dati personali di volta in volta applicabile;
- ⇨ mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente accordo ed alla vigente Normativa privacy, nonché consentire e contribuire alle attività di revisione, compresi gli audit, che il Titolare (con preavviso minimo di 5 giorni) potrà effettuare, direttamente o avvalendosi di terzi.

L'Esercente le funzioni di Titolare provvede a formalizzare, ai sensi dell'art. 28 del RGPD, le suddette responsabilità stipulando e manutenendo specifici accordi di nomina nell'ambito di contratti o convenzioni con i Responsabili del trattamento dei dati personali.

Il Responsabile del trattamento, in base agli accordi contrattuali o dietro specifica autorizzazione del Titolare rilasciata dall'Esercente le funzioni di Titolare, può nominare a sua volta soggetti terzi che effettuino trattamenti di dati personali nell'ambito delle attività per le quali è nominato Responsabile quale sub Responsabile. Il Responsabile (Sub Responsabile Esterno del Trattamento) così designato è tenuto a rispettare gli stessi obblighi stabiliti nel contratto stipulato tra il Titolare e il primo Responsabile, che rimane pienamente responsabile per il rispetto degli obblighi da parte del Sub Responsabile.

3.5.4 Amministratore di Sistema

L'Amministratore di Sistema, nominato dal Titolare o dal Responsabile del Trattamento, è il soggetto preposto alla gestione di sistemi informatici con i quali vengono effettuati i Trattamenti dei Dati Personali; a titolo esemplificativo sono considerati Amministratore di Sistema i soggetti che svolgono attività riconducibili alle mansioni di:

- ⇨ Amministratore di sistema operativo;
- ⇨ Amministratore di database;
- ⇨ Amministratore di applicazioni informatiche complesse;
- ⇨ Amministratore di rete;
- ⇨ Amministratore di sistemi di sicurezza.

Funzioni, compiti e responsabilità dell'Amministratore di Sistema:

- ⇨ monitorare lo stato dei sistemi di elaborazione e delle banche dati del MUR, con particolare e costante attenzione al profilo della sicurezza;
- ⇨ verificare che l'accesso ai sistemi e ai dati personali ivi contenuti sia debitamente protetto, nonché consentito solo quando strettamente necessario, nel pieno rispetto della legge e delle policy dell'amministrazione;
- ⇨ supportare l'Ufficio IT nella definizione ed implementazione di misure tecniche ed organizzative tali da garantire un livello di sicurezza adeguato al rischio, tra cui, a titolo esemplificativo: i) la pseudonimizzazione e la cifratura dei dati personali; ii) la capacità del Ministero di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi, oltre a quella di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico o di violazione dei dati; iii) l'esecuzione di controlli ed audit per testare, verificare e valutare regolarmente l'efficacia delle misure adottate per garantire la sicurezza dei trattamenti;
- ⇨ adempiere a tutti gli obblighi stabiliti dalla normativa vigente e dalle specifiche politiche adottate dal MUR;
- ⇨ garantire l'effettuazione degli interventi di manutenzione necessari sui database, sulle reti informatiche, sui sistemi di elaborazione e di software complessi;
- ⇨ garantire con continuità il corretto funzionamento dei sistemi di backup/recovery e, più in generale, la continuità dei servizi ICT;
- ⇨ sovrintendere all'operato di eventuali tecnici esterni che, a qualunque titolo, si trovino ad operare su sistemi o archivi di dati rientranti nel proprio perimetro di competenza;
- ⇨ gestire i sistemi di autenticazione e di autorizzazione, nonché l'assegnazione (e la disattivazione e l'aggiornamento in caso di modifiche e cambiamenti del ruolo) delle relative credenziali a tutti i dipendenti del MUR;
- ⇨ supportare il processo di rilevazione di qualsiasi violazione della sicurezza da cui possa derivare, in maniera accidentale o illecita, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati o conservati nei sistemi del MUR;
- ⇨ verificare la disattivazione delle credenziali di autenticazione in caso di mancato utilizzo per oltre 6 mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

3.6 RUOLI GESTIONALI

In questa sezione vengono identificati i ruoli/funzioni ministeriali individuati per la definizione del modello di gestione dei dati personali. Tali figure assumono un peso rilevante nell'ambito della protezione dei dati personali e del modello organizzativo e di gestione dei dati personali in quanto svolgono un ruolo di facilitazione e monitoraggio dell'implementazione dei requisiti normativi all'interno del MUR.

3.6.1 Esercenti le funzioni di Titolare del Trattamento

Con la Direttiva adottata il 08/01/2021 il MUR ha definito il proprio macro-assetto organizzativo e ha individuato come soggetti aventi per competenza le funzioni di Titolare i seguenti soggetti:

a) Capo di Gabinetto;
b) Segretario Generale;
c) Direttori Generali;
d) Presidente dell'Organismo indipendente di valutazione della performance del MUR.

Ai soggetti sopra indicati la Direttiva attribuisce esplicitamente una serie di compiti come meglio descritti dall'art. 2, comma 4, tra i quali quello di individuare all'interno della propria funzione organizzativa un "Referente privacy". Inoltre, il Direttore con funzioni di titolare del trattamento dovrà coinvolgere l'RPD tempestivamente e adeguatamente in tutte le questioni riguardanti la protezione dei dati personali

Funzioni, compiti e responsabilità dell'Esercente le funzioni di Titolare:

Salve ulteriori direttive del Segretario generale il Direttore Esercente le funzioni di Titolare deve provvedere a:

- ⇨ verificare che tutti i trattamenti ricadenti nella Direzione organizzativa allo stesso assegnata siano svolti conformemente agli obblighi di legge e alle prescrizioni dell'Autorità di Controllo. Relativamente agli Interessati, in particolare, dovrà assicurarsi che siano rispettati gli adempimenti che possono rendersi necessari in relazione alle specifiche circostanze, quali il prestare l'informativa, la raccolta del consenso, la gestione dell'esercizio dei diritti garantiti in favore degli interessati (soprattutto quando il trattamento abbia ad oggetto dati di natura sensibile);
- ⇨ coordinare le attività dei collaboratori (dipendenti, consulenti, collaboratori esterni, ecc.) che svolgono operazioni di trattamento sui dati personali all'interno della Direzione organizzativa assegnata e verificare che gli stessi quali "Autorizzati/Incaricati del trattamento" siano adeguatamente istruiti sugli obblighi da rispettare nello svolgimento delle attività a loro affidate;
- ⇨ supportare il Titolare nell'adozione di misure tecniche e organizzative per un livello di protezione dei dati personali trattati adeguato al rischio di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Tali misure includeranno l'applicazione del principio di protezione dei dati sin dall'inizio del trattamento e per impostazione predefinita nella definizione di specifici requisiti di progetto e la valutazione di impatto sulla protezione dei dati con eventuale parere dell'RPD e consultazione preventiva del Garante ove i trattamenti effettuati la richiedano;
- ⇨ cooperare con gli altri Esercenti le funzioni di Titolare e con il RPD nella tenuta del Registro dei trattamenti garantendone il tempestivo aggiornamento in relazione ad eventuali modifiche intervenute sia relativamente ai dati trattati, agli strumenti utilizzati alle eventuali terze parti coinvolte nel trattamento di dati personali svolti dalla Direzione /Uffici;
- ⇨ verificare il rispetto e la congruità dei tempi di conservazione in relazione ai dati personali trattati, garantendo che questi siano conformi alle prescrizioni normative applicabili nonché alla direttive interne adottate dal MUR;
- ⇨ assicurare il rispetto dei diritti riconosciuti agli interessati, quali il diritto di accesso ai dati, rettifica, cancellazione, portabilità, opposizione e limitazione al trattamento, nonché le procedure per la concreta

loro applicazione ove applicabili, soprattutto quando il trattamento abbia ad oggetto dati di natura particolare/sensibile o riferiti a minori o altri soggetti deboli;

- ⇨ prevedere l'inserimento di appropriate clausole contrattuali in ambito di sicurezza informatica e protezione dei dati nella definizione di rapporti con terze parti di propria competenza nei quali è previsto un trattamento di dati personali;
- ⇨ procedere alla individuazione e alla contrattualizzazione dei Responsabili del trattamento;
- ⇨ nell'ipotesi in cui si verifichi la necessità di effettuare un trasferimento di dati personali, in particolare se al di fuori dell'Unione Europea e dello Spazio Economico Europeo, l'Esercente le funzioni del Titolare, prima di effettuare il trasferimento, deve:
  - valutare, coinvolgendo il RPD, l'effettiva necessità di tale trasferimento, e che i dati da trasferire siano pertinenti e limitati a quanto strettamente necessario in relazione alle finalità che devono essere perseguite tenendo in debita considerazione le prescrizioni del Titolo V del RGPD;
  - effettuare per il trasferimento verso Paesi che non presentano garanzie adeguate per la protezione dei dati personali una specifica valutazione dei rischi sulla base delle indicazioni fornite dalla Commissione Europea con le clausole contrattuali standard adottate a giugno del 2021;
  - verificare che tali trasferimenti possano essere effettuati nel rispetto delle condizioni descritte al successivo paragrafo "Trasferimento all'estero";
- ⇨ verificare che idonee informazioni su tali trasferimenti siano incluse nella documentazione privacy ministeriale (ad esempio, nel registro delle attività di trattamento e nelle informative prestate agli interessati);
- ⇨ coinvolgere l'RPD:
  - ogni qualvolta si renda necessario il trattamento di categorie particolari di dati (es. dati relativi alla salute) o di dati giudiziari;
  - qualora si rilevino incongruenze tra la necessaria essenzialità e pertinenza dei dati trattati nel proprio ambito e le finalità perseguite al fine di valutare la necessità e/o opportunità di procedere alla cancellazione dei dati eccedenti;
  - al fine di provvedere tempestivamente ad eventuali richieste di esercizio dei diritti dell'interessato e informare l'RPD dell'evasione di quelle pervenute per il tramite del RPD;
  - nel caso in cui intervengano nuove esigenze di trattamento inizialmente non previste o vengano rilevate potenziali condizioni di non corretto adempimento delle prescrizioni normative per individuare le opportune azioni correttive;
  - qualora a fronte di difficoltà nell'individuare e adottare le misure di sicurezza adeguate al trattamento dei dati personali che si intende effettuare sia necessario, ai sensi dell'art. 36 del RGPD, avviare una consultazione preventiva dell'Autorità garante per la protezione dei dati personali;
- ⇨ favorire la sensibilizzazione dei dipendenti e collaboratori in merito all'attuazione del modello sulla protezione dei dati personali e della sicurezza nel trattamento dei dati personali con richiami informativi e con costante sollecitazione alla formazione individuale;

- ⇨ partecipare a riunioni periodiche di confronto con altri Esercenti le funzioni di Titolare, ed eventualmente con i soggetti terzi nominati Responsabili del Trattamento, per garantire un costante monitoraggio del loro operato e l'aggiornamento delle politiche di trattamento dei dati valutando eventuali necessarie variazioni nelle operazioni di trattamento dei dati nell'ambito della propria competenza;
- ⇨ mettere a disposizione del Segretario Senerale e dell'RPD tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di legge e contribuire alle attività di controllo e revisione interne, comprese le ispezioni da parte delle autorità competenti;
- ⇨ qualora, nell'ambito della propria Direzione, vengano adottati software/applicativi gestiti direttamente dalla propria U.O. (es. applicativi in cloud) l'Esercente le funzioni di Titolare dovrà attivare la cooperazione dell'Ufficio IT al fine di garantire la corretta integrazione con l'infrastruttura informatica del MUR e dare seguito a quanto necessario per la corretta attribuzione dei ruoli dei soggetti che opereranno sui sistemi con utenze amministrative/privilegiate come, ad esempio, per la gestione delle credenziali (creazione, modifica, dismissione). Tali soggetti dovranno, ricorrendone le condizioni, essere nominati Amministratori di Sistema da parte dell'Ufficio IT. Qualora invece, nell'ambito dell'adozione di tali software / applicativi, questi vengano gestiti direttamente da terze parti (es. fornitori), l'Esercente le funzioni di Titolare, dovrà richiedere agli stessi che sia reso disponibile, a richiesta, l'elenco dei soggetti che operano come Amministratori di Sistema sui software / applicativi impiegati nel trattamento dei dati personali nella titolarità del MUR.

3.6.2 Referente Interno IT

La Direzione Generale del Personale, del Bilancio e dei Servizi Strumentali ha la responsabilità della "Pianificazione strategica dei servizi IT, gestione infrastruttura, rete e sicurezza" affidata all'Ufficio VI - Pianificazione strategica dei servizi IT, gestione infrastruttura, rete e sicurezza, con l'assegnazione dei seguenti compiti:

- ⇨ definire, durante l'implementazione di nuovi sistemi/servizi informativi o la modifica di quelli esistenti, i requisiti di integrità, disponibilità, riservatezza e protezione dei Dati Personali applicando, fin dalle prime fasi di progettazione e per impostazione predefinita;
- ⇨ eseguire quanto previsto dalle procedure ministeriali in merito alla gestione di eventi di violazione dei Dati Personali e di anomalie che possano far presumere possibili compromissioni di tali dati supportando i Direttori con funzioni di titolare nella attività di rilevazione ed analisi degli eventi di sicurezza e collaborando con il RPD per i prescritti adempimenti relativi alla notifica al Garante e alla comunicazione all'Interessato laddove necessario;
- ⇨ supportare gli Esercenti le funzioni di Titolare che utilizzano nelle attività di trattamento i sistemi informativi dell'amministrazione con riferimento alla individuazione delle idonee misure di sicurezza rendendo disponibile la documentazione tecnica, le valutazioni di rischio, istruzioni e strumenti per l'utilizzo degli stessi;
- ⇨ implementare le misure di sicurezza definite per i sistemi informativi del Ministero anche al fine di garantire la tempestiva rilevazione di eventuali violazioni dei Dati Personali (Violazioni) prestando la

necessaria collaborazione al Titolare, ai Dirigenti designati ed al RPD, in caso di incidenti, per le valutazioni di severità dell'incidente, per l'analisi dei rischi per gli interessati, per l'individuazione delle opportune contromisure e per l'acquisizione degli elementi necessari per la notifica;

- ⇨ implementare le misure tecniche utili per la gestione della conservazione dei dati (tempi di conservazione), per l'esercizio dei diritti degli interessati (cancellazione, rettifica, estrazione, inibizione e limitazione al trattamento e portabilità dei dati), per la tenuta del registro dei trattamenti, per l'analisi di rischio e le valutazioni d'impatto, per la gestione dei consensi e, in generale della documentazione di riferimento;
- ⇨ implementare le misure di sicurezza a protezione dei dati personali (es. credenziali di autenticazione degli autorizzati/incaricati al trattamento, doppio fattore di autenticazione, gestione delle identità e delle autorizzazioni, etc.) ;
- ⇨ aggiornare periodicamente gli Esercenti le funzioni di Titolare e il RPD sullo stato di implementazione delle misure di sicurezza e di gestione dei Dati Personali;
- ⇨ supportare l'Esercente le funzioni di Titolare nell'individuazione e designazione degli amministratori di sistema interni garantendo un'adeguata attività di vigilanza;
- ⇨ garantire, nel rispetto della normativa, la raccolta, la conservazione protetta a norma di legge e il monitoraggio dei log relativi alle attività degli Amministratori di Sistema (login, logout, log relativi alle azioni di amministrazione effettuate).

3.6.3 Autorizzato/Incaricato del Trattamento

Gli Autorizzati/Incaricati (personale dipendente, collaboratori esterni, consulenti, etc.) che effettuano operazioni di Trattamento su Dati Personali, per conto del Ministero, sono designati dal Titolare o dagli Esercenti le funzioni di Titolare del Trattamento, ai sensi dell'art. 29 del RGPD e dell'art. 2 quaterdecies del D. lgs. 196/03. Ciascun Incaricato opera sulla base di istruzioni ricevute. Dette istruzioni sono formalizzate in documenti specifici, contengono istruzioni a seconda che il Trattamento riguardi Dati comuni o anche Dati Sensibili/Particolari e/o Giudiziari e sono aggiornate nel corso della durata del rapporto in ragione di specifiche necessità (cambio mansione, responsabilità, attività). Nella individuazione delle aree di attività attribuite agli Autorizzati si farà riferimento anche al DPCM nn. 164 e 165/2020 relativi all'organizzazione del MUR e al Decreto del MUR del 19 febbraio 2021 con il quale sono state individuate le responsabilità degli uffici di livello dirigenziale non generale ed ogni successiva modifica e integrazioni dei richiamati documenti.

Funzioni, compiti e responsabilità dell'Autorizzato/Incaricato del Trattamento:

- ⇨ trattare i dati in modo lecito e secondo correttezza;
- ⇨ trattare i dati esclusivamente al fine di adempiere alle attività assegnate e, in ogni caso, per scopi determinati, espliciti e, comunque, in termini compatibili con gli scopi di riservatezza per i quali i dati sono stati raccolti;
- ⇨ verificare costantemente la correttezza dei dati trattati e, ove necessario, provvedere al loro aggiornamento;

- ⇨ consegnare agli interessati, al momento della raccolta dei loro dati, il modulo contenente l'informativa sul trattamento;
- ⇨ trattare i dati personali in maniera tale che essi risultino pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Titolare o dall'Esercente le funzioni di Titolare;
- ⇨ trattare e custodire i dati personali, incluso quelli definiti particolari/sensibili, a cui si ha accesso nell'espletamento delle mansioni lavorative, garantendo l'adozione delle misure di sicurezza disposte dal Titolare e/o dall'Esercente le funzioni di Titolare, al fine di evitare la distruzione, la perdita o l'accesso non autorizzato da parte di terzi, anche tenendo conto della natura dei dati stessi;
- ⇨ astenersi dal creare nuove autonome banche dati senza preventiva autorizzazione del Titolare e/o dell'Esercente le funzioni di Titolare;
- ⇨ osservare scrupolosamente gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dei dati personali trattati;
- ⇨ garantire, in ogni operazione di trattamento, la massima riservatezza, astenendosi dal trasferire, comunicare e/o diffondere i dati a terzi, salvo preventiva autorizzazione del Titolare o dell'Esercente le funzioni di Titolare;
- ⇨ osservare scrupolosamente gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione tanto dei Dati Personali altrui trattati, quanto delle credenziali di autenticazione attribuite;
- ⇨ verificare che siano state adottate le misure per evitare l'accesso dei dati a terze parti durante l'allontanamento, anche temporaneo, dalla postazione di lavoro;
- ⇨ rispettare le istruzioni e le procedure adottate relativamente allo svolgimento dell'attività lavorativa in "modalità agile";
- ⇨ astenersi dal comunicare a terzi (inclusi colleghi o comunque appartenenti al Ministero) in qualsiasi forma, le credenziali di autenticazione logica, necessarie per il trattamento dei Dati Personali con strumenti elettronici;
- ⇨ segnalare al Titolare eventuali situazioni di rischio per la sicurezza dei dati.

3.6.4 Autorizzati/Incaricati con specifiche mansioni

Autorizzati/Incaricato alla Videosorveglianza

L'autorizzato/incaricato alla Videosorveglianza è la persona fisica autorizzata dal Titolare o dall'Esercente le funzioni di Titolare, a compiere operazioni di Trattamento sulle immagini rilevate in tempo reale o registrate dai sistemi di videosorveglianza presenti presso le sedi del Ministero.

È possibile che le attività inerenti alla gestione dell'impianto di videosorveglianza venga affidata ad un soggetto esterno che viene autorizzato a compiere operazioni di trattamento delle immagini avendo sottoscritto l'Atto di designazione a Responsabile del trattamento, parte integrante del contratto di servizio con il MUR.

4 MODELLO DI GESTIONE DEI DATI PERSONALI

L'Architettura logico-funzionale del modello di gestione dei dati personali del MUR è caratterizzata dai seguenti elementi:

- ✓ Modalità operative relative al trattamento dei dati personali:
  - Raccolta;
  - Trattamento;
  - Cessazione del trattamento e cancellazione.
- ✓ Gestione dei diritti degli interessati.
- ✓ Protezione dei dati sin dalla progettazione del trattamento e protezione per impostazione predefinita
- ✓ Valutazione d'impatto sulla protezione dei dati (VIP - DPIA).
- ✓ Registro del Trattamenti dei dati.
- ✓ Gestione degli eventi di violazione dei dati.
- ✓ Gestione dei rapporti con il Garante.
- ✓ Formazione ed informazione interna.
- ✓ Audit.
- ✓ Sanzioni.

4.1 MODALITÀ OPERATIVE RELATIVE AL TRATTAMENTO DEI DATI PERSONALI

Le operazioni di Trattamento dei Dati Personali devono essere strettamente limitate a quanto necessario a perseguire le finalità indicate nell'informativa e, in ogni caso, compatibili con dette finalità.

Di seguito sono riportate le fasi del ciclo di vita naturale del Dato Personale al cui interno sono dettagliate le modalità di gestione operativa:

- ⇨ Raccolta;
- ⇨ Trattamento;
- ⇨ Cessazione del Trattamento e Cancellazione.

4.1.1 Raccolta

I Dati Personali (tra cui in particolare dati anagrafici, di contatto) possono essere acquisiti dal Ministero anche attraverso il sito Istituzionale. Gli altri dati vengono acquisiti direttamente dal Ministero ovvero attraverso la messa a disposizione da parte di altre Amministrazioni dello Stato o Soggetti privati sulla base di previsioni normative nazionale ed europee o di contratti/accordi sottoscritti dal MUR.

Finalità

Il Trattamento dei Dati Personali (raccolti quale Titolare o ricevuti quale Esercente le funzioni di Titolare del Trattamento) da parte del Ministero deve avvenire per il perseguimento di finalità legittime previamente individuate.

Informativa

Sulla base dei requisiti normativi sulla protezione dei dati personali l'informativa relativa al Trattamento dei Dati Personali dell'interessato deve contenere almeno i seguenti elementi:

- ✓ gli estremi identificativi del Titolare;
- ✓ le finalità del Trattamento;
- ✓ la base giuridica sulla quale poggia il trattamento;
- ✓ le categorie dei Dati Personali trattati;
- ✓ l'obbligatorietà o meno del conferimento dei Dati Personali e le conseguenze di un eventuale rifiuto;
- ✓ l'identificazione dei destinatari o le eventuali categorie dei destinatari;
- ✓ il periodo di conservazione oppure i criteri utilizzati per determinarlo;
- ✓ le modalità di contatto con il Titolare (anche al fine di esercitare i diritti di cui al punto successivo);
- ✓ l'esistenza dei diritti riconosciuti all'Interessato;
- ✓ il diritto di proporre reclamo all'Autorità di protezione dei dati personali;
- ✓ l'eventuale esistenza di un processo decisionale automatizzato, le logiche applicate e le conseguenze per l'interessato;
- ✓ la previsione di un separato consenso per ulteriori finalità individuate dal Titolare.;
- ✓ la fonte dalla quale sono acquisiti i dati nel caso non sia fornita direttamente dall'interessato.

L'informativa deve essere sempre fornita all'Interessato al momento della raccolta dei Dati Personali o, al più tardi, entro un mese dall'acquisizione, se avvenuta presso terzi, ed in particolare nei casi di seguito specificati (elencazione non esaustiva):

- ✓ assunzione di dipendenti (incluse tutte le forme di collaborazione in uso);
- ✓ utilizzo di sistemi di videosorveglianza e, più in generale, in occasione del controllo accessi presso il Ministero;
- ✓ richieste di informazioni/contatto attraverso il modulo presente nel sito del Ministero;
- ✓ accreditamento dei professionisti esterni.

Il trattamento di dati personali è consentito soltanto dopo che gli Interessati siano stati adeguatamente informati salvo che non ricorrano condizioni di esclusione previste dal Regolamento come ad esempio se:

- ✓ le informazioni sono già in possesso dell'interessato;
- ✓ la comunicazione delle informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato ed in particolare per il trattamento ai fini di archiviazione nel pubblico interesse. In tale circostanza il Titolare dovrà tuttavia adottare misure appropriate per tutelare i diritti e i legittimi interessi dell'interessato.

Il Consenso

Il Titolare del trattamento potrebbe utilizzare il consenso da parte dell'interessato come base giuridica in limitate circostanze da valutare di volta in volta.

La raccolta del consenso dovrà avvenire nelle forme e con le modalità previste dal RGPD dovendo rispettare l'esigenza che sia dimostrabile, ossia che vi siano elementi che permettano di aver contezza che il consenso sia stato effettivamente prestato.

Il consenso espresso degli Interessati sarà, ove costituisca la base giuridica, indispensabile per poter effettuare il Trattamento.

Il consenso viene ritenuto valido qualora rispetti i seguenti requisiti:

- ✓ Informato: il consenso deve essere preceduto dalla consegna o, in ogni caso, dalla presa visione da parte dell'Interessato dell'informativa;
- ✓ Specifico: ciascuna operazione di Trattamento che, in mancanza di un diverso presupposto di legittimità del Trattamento, necessiti del consenso degli Interessati deve essere oggetto di uno specifico consenso;
- ✓ Espresso: l'intenzione dell'Interessato di prestare il proprio consenso alle operazioni di Trattamento che lo riguarderanno deve essere espressa tramite una chiara ed univoca manifestazione di volontà;
- ✓ Libero: l'Interessato dovrà essere sempre messo in condizione di poter rifiutare di prestare il proprio consenso allo svolgimento di determinate operazioni di Trattamento;
- ✓ Documentato: l'avvenuta prestazione del consenso da parte di ciascun Interessato potrà essere raccolta anche oralmente ma dovrà essere documentata in forma cartacea o digitale. Per quanto riguarda il caso del trattamento di dati particolari/sensibili o giudiziari, per i quali è necessaria una previa condizione di legittimità al loro trattamento, di norma è necessario il consenso da parte dell'interessato, salvo che non ricorrano casi di esclusione (es. nel rapporto di lavoro, CV spontanei, etc).

Affinché il consenso sia ritenuto valido è necessario che i seguenti elementi siano stati forniti all'interessato:

- ✓ l'identificativo del Titolare;
- ✓ la finalità del trattamento subordinato al consenso;
- ✓ la categoria di dati personali oggetto del trattamento;
- ✓ la possibilità di revocare il consenso;
- ✓ l'indicazione dei potenziali rischi derivanti da possibili trasferimenti di dati extra-UE in assenza di apposite decisioni di adeguatezza.

Gli Interessati che abbiano prestato il consenso allo svolgimento di determinate operazioni di Trattamento hanno sempre la facoltà di revocarlo successivamente. Nella suddetta ipotesi, le operazioni di Trattamento svolte in virtù di tale consenso dovranno essere prontamente interrotte salvo che non ricorrano specifiche condizioni.

Di norma il consenso non è considerata una base giuridica applicabile ai trattamenti effettuati dalla Pubblica Amministrazione salvo limitate situazioni che devono essere puntualmente analizzate per verificare che sia possibile il suo impiego.

4.1.2 Trattamento

Principi Generali

Le operazioni di Trattamento effettuate dal Ministero devono attenersi ai principi generali riportati di seguito:

- ✓ liceità, correttezza e trasparenza: i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato;
- ✓ limitazione delle finalità: i dati devono essere raccolti per finalità determinate, esplicite e legittime ed utilizzati in altre operazioni del trattamento in termini compatibili con tali finalità (le finalità devono essere rese note nell'informativa);
- ✓ minimizzazione dei dati: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- ✓ esattezza: i dati devono essere esatti e, se necessario, aggiornati. Sarà necessario adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- ✓ limitazione della conservazione: i dati devono essere conservati in una forma che consenta l'identificazione dell'Interessato per un periodo di tempo non superiore a quello necessario alle finalità per le quali sono stati trattati;
- ✓ integrità e riservatezza: i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei Dati Personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Trattamento effettuato da terze parti

Per Trattamento di Dati Personali effettuato da Terze Parti, si intendono tutte le casistiche in cui Dati Personali nella titolarità del Ministero sono trattati da soggetti terzi designati Responsabili del Trattamento.

Le Terze Parti che agiscono quali Responsabili del Trattamento dovranno rispettare gli obblighi previsti dal RGPD e formalizzati attraverso l'Atto di Designazione sottoscritto dalle parti (nel seguito vengono forniti maggiori dettagli sugli obblighi del Responsabile).

Resta inteso che il Titolare sarà, in ogni caso, autorizzato a comunicare le informazioni relative al Responsabile designato a seguito di un'espressa richiesta in tal senso da parte delle autorità giudiziarie o amministrative competenti o, in ogni caso, laddove una simile comunicazione sia prevista dalla normativa in materia di protezione dei Dati Personali.

Nella suddetta ipotesi, le Terze Parti devono essere nominate: (i) Responsabili del trattamento, oppure, se persone fisiche, (ii) Autorizzati/Incaricati, nel caso in cui effettuino i trattamenti sotto la direzione ed il controllo del Titolare o di un referente interno. Nel caso in cui le Terze Parti agiscano quali Responsabili del Trattamento, dovranno sottoscrivere lo specifico Atto di designazione ai sensi dell'art. 28 del RGPD e ricevere istruzioni scritte come già sopra indicato.

Trasferimento all'estero

Il trasferimento di Dati Personali all'estero, da intendersi come ogni ipotesi in cui i Dati Personali siano trattati da un soggetto (fornitore, autorità straniera, etc.) che risiede in uno Stato estero, non appartenente all'Unione Europea o allo Spazio Economico Europeo (SEE), può avvenire solo al fine di perseguire la finalità comunicata all'Interessato e in conformità alle specifiche disposizioni riguardanti il trasferimento di Dati Personali all'estero previste dalla normativa applicabile.

Come previsto dal Titolo V del RGPD, il trasferimento dei Dati Personali dell'Interessato in Paesi esteri può avvenire esclusivamente al ricorrere di una delle seguenti condizioni:

- ⇨ se il Paese terzo garantisce un adeguato livello di protezione dei Dati Personali, come ad esempio per i Paesi facenti parte dell'Unione Europea o per i Paesi extra UE che sono stati oggetto di una decisione di adeguatezza da parte della Commissione Europea;
- ⇨ se risulta presente una delle garanzie adeguate previste dall'art. 46 del RGPD (es. le clausole contrattuali standard approvate dalla Commissione Europea, o norme vincolanti di impresa). In tal caso, a seguito della sentenza "Schrems II" (causa C-311/18 – Data Protection Commissioner v Facebook Ireland e Maximillian Schrems) della Corte di Giustizia dell'Unione Europea (CGUE) e, come chiarito dall'European Data Protection Board nelle Raccomandazioni 01/2020 relative alle "misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE", è necessario:
    - effettuare una valutazione sul livello di protezione dei dati trasferiti, verificando che lo strumento giuridico identificato per il trasferimento sia idoneo in concreto a proteggere i dati personali rispetto alla legge o prassi del paese terzo;
    - identificare ed adottare eventuali misure tecniche, organizzative e/o contrattuali aggiuntive;
    - eseguire periodicamente la valutazione del livello di protezione dei dati trasferiti.

Si evidenzia che, in tale contesto, qualora venissero utilizzate le clausole contrattuali standard, è necessario fare riferimento alla versione aggiornata delle stesse, contenuta nella Decisione di esecuzione (UE) 2021/914 della Commissione Europea del 4 giugno 2021 relativa alle clausole contrattuali tipo (anche "SCC") per il trasferimento di dati personali verso paesi terzi a norma del RGPD nonché delle FAQ sulle SCC pubblicate dalla Commissione Europea a maggio 2022:

- ⇨ trasferimento disposto da una sentenza di un'Autorità giurisdizionale o una decisione di un'Autorità amministrativa di un Paese Terzo, solo in presenza di un accordo internazionale in vigore con il Paese Terzo richiedente;
- ⇨ presenza di una delle deroghe previste dall'art. 49 del RGPD. (per esempio, qualora l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato). In tale ipotesi, tuttavia, è necessario seguire le Linee guida 2/2018 su tali deroghe, secondo le quali occorre interpretare le deroghe in maniera restrittiva ed utilizzarle sulla base di un test di necessità, a seguito del quale il soggetto che intende trasferire i dati personali deve valutare se il trasferimento di dati personali possa essere considerato necessario per la finalità specifica.

Al fine di garantire il rispetto delle condizioni sopra previste, nell'ipotesi in cui si verifichi la necessità di effettuare un trasferimento di dati personali al di fuori dell'Unione Europea e dello Spazio Economico Europeo, l'Esercente le funzioni di Titolare competente, prima di effettuare il trasferimento, deve:

- valutare, anche con il supporto del DPO l'effettiva necessità di tale trasferimento, e che i dati da trasferire siano adeguati, pertinenti e limitati a ciò che è necessario in relazione alle finalità per le quali devono essere trasferiti e trattati nel paese terzo; si specifica che non sono ammessi trasferimenti di dati personali all'estero se non in ipotesi strettamente limitate e per ragioni adeguatamente motivate;
- verificare che tali trasferimenti possano essere effettuati nel rispetto delle condizioni sopra elencate;
- verificare che idonee informazioni su tali trasferimenti siano incluse nella documentazione in materia di protezione dei dati personali del Ministero (ad esempio, nel registro delle attività di trattamento e nelle informative prestate agli Interessati).

Web Cookie

I siti web utilizzano la tecnologia dei c.d. cookie per fornire un migliore servizio agli utenti.

I cookie sono stringhe di testo che i siti web visitati dall'utente ovvero siti o web server diversi (cd. "terze parti") posizionano ed archiviano all'interno di un dispositivo terminale nella disponibilità dell'utente medesimo (per esempio, un computer, un tablet, uno smartphone). I cookie possono essere classificati in base alla loro durata (di sessione o permanenti) e dal punto di vista soggettivo (a seconda che siano impiegati dal soggetto che esercisce il sito web, "prima parte", o agisca autonomamente o per conto della "terza parte"). I cookie possono inoltre essere distinti in ragione della loro funzione, nel modo seguente:

- ⇨ cookie tecnici: utilizzati al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio. Si tratta di cookie che, per esempio, consentono la normale navigazione di un sito Web e la rendono ottimale per ogni singolo utente, in quanto salvano le preferenze e i criteri di navigazione;
- ⇨ cookie analitici: utilizzati, tra l'altro, per valutare l'efficacia di un servizio della società dell'informazione fornito da un publisher, per la progettazione di un sito web o per contribuire a misurarne il "traffico", cioè il numero di visitatori anche eventualmente ripartiti per area geografica, fascia oraria della connessione o altre caratteristiche.

Tali cookie, sono equiparabili ai cookie tecnici solo se:

- vengono utilizzati unicamente per produrre statistiche aggregate riferibili ad un singolo sito / applicazione;
- vengono mascherate, per quelli di terze parti, le ultime cifre dell'indirizzo IP (la quarta componente 111.111.111.***);

- le terze parti si astengono dal combinare i cookie analytics, così minimizzati, con altre informazioni o dal trasmetterli ad ulteriori terzi.

Qualora tali cookie analitici non siano equiparabili ai cookie tecnici, dovranno essere ricompresi tra quelli di marketing e profilazione.

⇨ cookie di marketing e profilazione, utilizzati per ricondurre a soggetti determinati, identificati o identificabili, specifiche azioni o schemi comportamentali ricorrenti nell'uso delle funzionalità offerte (modelli) al fine del raggruppamento dei diversi profili all'interno di gruppi omogenei di diversa ampiezza, in modo che sia possibile al Titolare, tra l'altro, anche modulare la fornitura del servizio in modo sempre più personalizzato al di là di quanto strettamente necessario all'erogazione del servizio, nonché inviare messaggi pubblicitari mirati, cioè in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete.

⇨ cookie dei social media: i cookie possono essere utilizzati anche, per esempio, per condurre attività di marketing attraverso l'impiego di tecniche di profilazione o tracciamento che registrano le preferenze dei visitatori nell'ambito della navigazione sul sito Web o canale social. Tali cookie possono essere assimilati ai cookie di profilazione.

Il trattamento di dati personali tramite cookie deve essere considerato al fine di una corretta gestione dei siti web del Ministero. A tal proposito, a seconda della tipologia di cookie utilizzati si dovrà verificare il rispetto dei seguenti requisiti (così come previsto dalle linee guida cookie e altri strumenti di tracciamento- provvedimento del Garante per la protezione dei dati personali datato 10 Giugno 2021- Doc. web 9677876):

- richiedere il consenso all'utilizzo di tutte le tipologie di cookie, ad eccezione dei cookie tecnici e/o analitici aggregati assimilabili ai cookie tecnici. Il consenso potrà intendersi come validamente prestato soltanto se sarà conseguenza di un intervento attivo e consapevole dell'utente, opportunamente riscontrabile e dimostrabile che consenta di qualificarlo come in linea con tutti i requisiti (libero, informato, inequivoco e specifico, cioè espresso in relazione a ciascuna diversa finalità del trattamento) richiesti dal RGPD;
- verificare che il consenso sia conseguenza di un'azione positiva e consapevole che sia riscontrabile e dimostrabile (es. click sull'apposito pulsante presente all'interno del banner). Tale banner dovrà contenere, oltre alla X, almeno le seguenti indicazioni e opzioni:
  - l'avvertenza che la chiusura del banner mediante selezione dell'apposito comando contraddistinto dalla X posto al suo interno comporta il permanere delle impostazioni di default e quindi la continuazione di navigazione in assenza di cookie o altri strumenti di tracciamento diversi da quelli tecnici;
  - una informativa minima relativa al fatto che il sito utilizza – se realmente impiegati - cookie o altri strumenti tecnici e potrà, esclusivamente previa acquisizione del consenso dell'utente da prestarsi con modalità da indicarsi nella medesima informativa breve (cfr. punto iv che segue), utilizzare anche cookie di profilazione o altri strumenti di tracciamento al fine di inviare messaggi pubblicitari ovvero di modulare la fornitura del servizio in modo personalizzato al di là di quanto strettamente necessario alla sua erogazione, cioè in linea con le preferenze manifestate dall'utente stesso

nell'ambito dell'utilizzo delle funzionalità e della navigazione in rete e/o allo scopo di effettuare analisi e monitoraggio dei comportamenti dei visitatori di siti web;

- il collegamento alla privacy policy, ovvero ad una informativa estesa posizionata in un second livello – che sia accessibile con un solo click anche tramite un ulteriore collegamento posizionato nel piè di pagina di qualsiasi pagina del dominio cui l'utente accede - ove vengano fornite in maniera chiara e completa almeno tutte le indicazioni di cui all'art 13 del RGDP, anche con riguardo ai predetti cookie o altri strumenti tecnici (cfr., al riguardo, il successivo paragrafo 8);
- un comando attraverso il quale sia possibile esprimere/revocare il proprio consenso accettando il posizionamento di tutti i cookie o l'impiego di eventuali altri strumenti di tracciamento;
- il collegamento ad una ulteriore area dedicata nella quale sia possibile selezionare, in modo analitico, soltanto le funzionalità, i soggetti cd. terze parti - il cui elenco deve essere tenuto costantemente aggiornato, siano essi raggiungibili tramite specifici link ovvero anche per il tramite del link al sito web di un soggetto intermediario che li rappresenti - ed i cookie, anche eventualmente raggruppati per categorie omogenee, al cui utilizzo l'utente scelga di acconsentire.

Al fine di garantire la conformità alla normativa applicabile, nel caso ricorra l'esigenza di creare un nuovo sito web è necessario in via preliminare:

- ⇨ comunicare al RPD la volontà di procedere all'apertura di un nuovo sito/sezione web, al fine di ricevere adeguate indicazioni in merito agli adempimenti privacy a cui provvedere;
- ⇨ avvalersi del supporto dell'Ufficio IT per lo sviluppo del nuovo sito/sezione web, al fine di garantire uniformità con i modelli e le policy del Ministero.

Sicurezza

Nell'ambito delle operazioni di Trattamento svolte, il Titolare, anche attraverso l'Esercente le funzioni di Titolare, deve porre in essere tutte le misure necessarie per tutelare i Dati Personali, dovendo garantire:

- ⇨ la confidenzialità, integrità e disponibilità dei Dati Personali trattati;
- ⇨ il test e la valutazione periodica di efficacia delle procedure e delle misure implementate;
- ⇨ l'implementazione di misure di protezione delle reti, dei sistemi e dei software con le quali vengono trattati i Dati Personali, quali ad esempio:
  - la pseudonimizzazione, l'offuscamento e la cifratura dei Dati Personali;
  - soluzioni di continuità di servizio in grado di garantire la disponibilità e l'integrità dei dati (backup, Disaster Recovery, ecc.);
- ⇨ la definizione di clausole contrattuali finalizzate a vincolare le terze parti al rispetto delle eventuali misure di sicurezza aggiuntive richieste dal Ministero;
- ⇨ l'applicazione del principio di Data Protection by design e by default nella progettazione dei sistemi e nel disegno dei processi e delle procedure aziendali;
- ⇨ l'implementazione di soluzioni in grado di rilevare tentativi non leciti di accesso ai Dati Personali in grado di garantire il rispetto delle prescrizioni del RGPD in merito alle violazioni dei dati personali.

- ⇨ l'adozione di soluzioni per il tracciamento delle attività effettuate sui Dati Personali che siano compatibili con i requisiti imposti dalle normative applicabili.

Trattamenti Specifici

Attività degli Amministratori di Sistema

Un provvedimento generale del Garante prescrive l'adozione di specifici accorgimenti, misure tecniche ed organizzative riguardanti le figure degli Amministratori di Sistema, nel cui novero rientrano anche i Data-Base e Network Administrator ossia tutte quelle figure che sono dotate, in ragione delle attività chiamate a svolgere, di privilegi di accesso ai sistemi informativi estremamente ampi.

Nel richiamato provvedimento il Garante ha mirato a creare una condizione di consapevolezza in ordine alla rilevanza del ruolo di queste figure professionali fornendo una serie di prescrizioni destinate alla totalità dei Titolari. Avendo a riferimento tali obblighi il Ministero deve assolvere a tali adempimenti mediante l'attuazione di adeguate misure riguardanti l'operato degli Amministratori di Sistema, mediante:

- ⇨ l'implementazione di un processo di selezione delle risorse che preveda la valutazione delle caratteristiche soggettive di esperienza, capacità e affidabilità delle persone chiamate a ricoprire il ruolo di Amministratore di Sistema;
- ⇨ designazioni individuali degli Amministratori di Sistema tramite lettera di nomina, con l'elencazione analitica degli ambiti di operatività consentiti coerente al profilo di autorizzazione assegnato;
- ⇨ la predisposizione dell'elenco degli Amministratori di Sistema e delle funzioni loro attribuite, riportante gli estremi identificativi e gli ambiti di operatività delle persone fisiche configurate come Amministratori di Sistema. Nel caso dei sistemi che trattano dati dei Dipendenti, tale elenco deve essere reso disponibile/conoscibile a tutto il Personale;
- ⇨ la verifica periodica dell'attività degli Amministratori di Sistema, eseguita al fine di controllare la rispondenza delle attività da questi realizzate ai compiti assegnati ed agli ambiti di operatività consentiti.
- ⇨ la designazione degli Amministratori di Sistema può anche essere demandata al Responsabile Esterno (per quanto di competenza) ed in tal caso questi dovrà dare applicazione puntuale a quanto previsto e rendere disponibile, a richiesta del Titolare, la lista dei nominativi nonché le evidenze dei controlli periodici effettuati.

Videosorveglianza

Il Ministero, in qualità di Titolare, effettua un Trattamento di Dati Personali tramite sistemi di videosorveglianza presso le proprie sedi e pertanto è tenuto all'adozione delle prescrizioni normative applicabili in materia di videosorveglianza al fine di garantire il rispetto dei diritti e delle libertà fondamentali, nonché della dignità delle persone, con particolare riferimento alla riservatezza ed all'identità personale, in attuazione e nei limiti di quanto stabilito dallo specifico provvedimento del Garante sulla videosorveglianza (Provvedimento del Garante in materia di videosorveglianza – 8 Aprile 2010) nonché le Linee Guida 3/2019 dell'EDPB e le FAQ del Garante del dicembre 2020.

Per approfondimenti in merito alle principali misure tecniche ed organizzative adottate ai fini degli adempimenti richiesti dal citato provvedimento in materia di videosorveglianza, si rimanda allo specifico documento "Procedura Gestione Videosorveglianza" .

4.1.3 Gestione della Conservazione dei dati

In conformità alle norme ed ai regolamenti in materia, il Ministero definisce i termini di conservazione dei dati raccolti sulla base dei seguenti aspetti:

- ⇨ principio di accountability, mediante il quale è stata eseguita un'analisi dei requisiti normativi di conservazione di dati e circa le esigenze di business sui dati personali per i quali non sono stati definiti dei tempi di conservazione;
- ⇨ principio di minimizzazione attraverso il quale viene garantito che il trattamento dei dati personali avvenga esclusivamente in maniera pertinente rispetto alla finalità definite e per il periodo strettamente necessario all'esecuzione delle attività per il quale i dati sono stati raccolti.

Quanto detto si applica a tutti i dati personali trattati nell'ambito del Ministero e a tutte le seguenti categorie di interessati:

- o dipendenti;
- o studenti;
- o docenti;
- o fornitori Esterni;
- o terze parti con le quali il Ministero ha formalizzato dei rapporti contrattuali e/o di collaborazione;

Si richiamano, inoltre, tutte le normative di dettaglio che individuino specifici termini di conservazione dei Dati Personali (es. obblighi di conservazione fiscali, civilistici, archiviazione nel pubblico interesse, ricerca storica, ecc.).

4.1.4 Cessazione del Trattamento e cancellazione dei dati personali

Nel caso in cui il Ministero intenda cessare lo svolgimento di una o più operazioni di Trattamento, i Dati Personali precedentemente utilizzati nel contesto di tali operazioni dovranno essere distrutti, fatti salvi gli adempimenti legati ad obblighi di legge o a finalità difensive.

Nel caso di cessazione di trattamenti di dati personali da parte di Responsabili, per qualsiasi causa, questi saranno tenuti, a discrezione del Titolare a:

- ⇨ restituire al Titolare i dati personali oggetto del trattamento;
- ⇨ provvedere alla loro integrale distruzione, salvi i casi in cui la conservazione di tali dati sia espressamente richiesta da norme di legge (contabili, fiscali, etc.).

In entrambi i casi il Responsabile provvederà a rilasciare al Titolare apposita dichiarazione avente ad oggetto l'avvenuta restituzione o eliminazione di tutti i dati ricevuti in esecuzione del Contratto. Il Titolare ha la facoltà

di verificare l'implementazione delle misure per la protezione dei dati personali tramite apposite verifiche nei confronti di terze parti che agiscono in qualità di Responsabile del Trattamento.

4.2 GESTIONE DIRITTI INTERESSATO

In conformità con quanto previsto dal RGPD, il Ministero garantisce il riconoscimento dei seguenti diritti agli interessati:

- ⇨ Diritto di accesso (art. 15 del RGPD): l'interessato ha il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso;
- ⇨ Diritto di rettifica (art. 16 del RGPD): l'interessato ha il diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano o l'integrazione dei dati personali incompleti tenendo conto delle finalità del trattamento;
- ⇨ Diritto alla cancellazione (art. 17 del RGPD): l'interessato ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano. Si consideri che non possono essere eliminati i dati il cui mantenimento è giustificato o reso necessario ai fini di legge (ad es. nel caso in cui un interessato chieda la cancellazione, ma sia in essere un contenzioso tra questo e il Ministero, quest'ultima è legittimata a conservare i dati dell'interessato, nonostante la richiesta);
- ⇨ Diritto di limitazione del trattamento (art. 18 del RGPD): l'interessato ha il diritto di ottenere la limitazione del trattamento nei seguenti casi:
    - o l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al Titolare per verificare l'esattezza dei dati personali;
    - o il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
    - o i dati personali sono necessari per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
    - o l'interessato si è opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.
- ⇨ Diritto alla portabilità dei dati (art. 20 del RGPD): l'interessato ha il diritto di ricevere, ove applicabile al contesto di raccolta dei dati, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano e ha il diritto di trasmetterli ad un altro Titolare del Trattamento senza impedimenti (ove applicabile al trattamento effettuato);
- ⇨ Diritto di opposizione (art.21 del RGPD): l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano per alcune o per tutte le finalità per cui sono stati raccolti. L'interessato ha, in particolare, il diritto di modificare i consensi e successivamente inibire qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

- ⇨ Diritto di non essere sottoposto ad un processo decisionale automatizzato (art. 22 del RGPD): l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Per ognuno dei suddetti diritti, il Titolare deve fornire riscontro all'Interessato senza ingiustificato ritardo e comunque entro 30 giorni ai sensi dell'art. 12 c. 3 del RGPD (ed in casi complessi ulteriori due mesi dalla ricezione della richiesta), giustificando all'Interessato eventuali ritardi o inadempienze nel fornire il riscontro, entro il termine di 30 giorni.

4.3 VALUTAZIONE D'IMPATTO - DATA PROTECTION BY DESIGN E BY DEFAULT (DPIA)

Con il fine ultimo di implementare soluzioni di progettazione dei sistemi informativi e dei prodotti e servizi offerti, inclusi le forme di proposizione commerciale, gli strumenti di condivisione di contenuti, e di servizi online, etc., in grado di proteggere i Dati Personali durante tutte le fasi del ciclo di vita, il Titolare mette in atto misure tecniche e organizzative, quali la cifratura, volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di dare attuazione al concetto di "responsabilizzazione" (accountability) che il RGPD ha posto come paradigma e come principale prescrizione alla quale il Titolare deve dare concreta attuazione.

La protezione dei dati fin dalla progettazione (data protection by design) deve, tra l'altro:

- ⇨ essere integrata all'interno del ciclo di vita dei processi/sistemi/applicativi nei quali vengono trattati Dati Personali;
- ⇨ considerare l'intero ciclo di vita dei Dati Personali dalla raccolta alla cancellazione tenendo in debita considerazione anche il trasferimento, la conservazione, l'elaborazione, la consultazione e la comunicazione;
- ⇨ salvaguardare la confidenzialità, integrità e disponibilità dei Dati Personali trattati.

La protezione secondo i principi di impostazione predefinita (data protection by default) deve, tra l'altro:

- ⇨ prevedere per impostazione predefinita dei processi/sistemi che vengano trattati solo i Dati Personali necessari per ogni specifica finalità del trattamento;
- ⇨ prevedere, per impostazione predefinita dei processi/sistemi, che i Dati Personali trattati non siano resi accessibili a un numero indefinito di persone fisiche senza una reale esigenza. I principi di Data Protection by Design e by Default devono essere integrati nell'intera organizzazione del Ministero, pertanto tutte le funzioni organizzative dovranno prestare attenzione a che lo sviluppo di nuove procedure informatiche o servizi, e l'utilizzo di strumenti di supporto venga sottoposta ad una preventiva verifica al fine di valutare se l'eventuale trattamento dei dati previsto avvenga nel rispetto delle previsioni normative: ciò richiede che vi sia una estrema consapevolezza che ciascuna Direzione dovrà fornire il proprio contributo alla corretta e tempestiva applicazione dei principi richiamati. L'applicazione di tali principi deve inoltre essere monitorata e supervisionata dal DPO.

Per quanto riguarda il c.d. Valutazione d'Impatto o Data Protection Impact Assessment (DPIA), quando un tipo di trattamento, in particolare se prevede l'uso di nuove tecnologie, presenta un rischio elevato per i diritti e le libertà degli Interessati, il Titolare esegue, prima di procedere al trattamento, una valutazione dell'impatto del trattamento sui Dati Personali in riferimento ai diritti e alla libertà degli Interessati, con particolare riguardo al loro diritto alla protezione dei Dati Personali.

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

4.4 REGISTRO DEL TRATTAMENTO DEI DATI

L'elenco completo delle attività di trattamento di dati personali e delle relative finalità è contenuto all'interno del "Registro dei Trattamenti dei dati personali". Il Ministero ha individuato uno strumento con il quale garantire la gestione on-line del registro. Ciascun Esercente le funzioni di Titolare alla compilazione ed al successivo aggiornamento della quota parte di Registro contenete i trattamenti riferiti alla propria area di competenza anche per il tramite dei Referenti privacy individuati. L'Esercente le funzioni di Titolare, o il proprio Referente privacy, si avvale della consulenza del DPO che ha anche il compito di coordinare l'aggiornamento (almeno annuale) del Registro.

Ogni Esercente le funzioni di Titolare, anche per il tramite del proprio Referente privacy, deve garantire che siano rispettati i requisiti minimi delle informazioni che il Registro dei Trattamenti dovrà includere che, nella versione del Titolare, deve contenere almeno:

- ✓ il nome e i dati di contatto:
  - del Titolare del trattamento;
  - del RPD;
  - ove applicabile, del Contitolare del trattamento;
  - ove applicabile (nel caso in cui il Titolare risieda al di fuori dell'UE) del Rappresentante del Titolare del trattamento;
  - del Referente o dei Referenti Interni del Trattamento;
- ✓ le finalità del trattamento;
- ✓ le basi giuridiche del trattamento; in caso di trattamenti di "categorie particolari di dati", occorre indicare una delle condizioni di cui all'art. 9, par. 2 del RGPD;

- ✓ in caso di trattamenti di dati relativi a condanne penali e reati, occorre riportare la specifica normativa (nazionale o dell'Unione europea) che ne autorizza il trattamento;
- ✓ una descrizione delle categorie di interessati e delle categorie di dati personali;
- ✓ le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ✓ ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;
- ✓ ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ✓ ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

Nel caso in cui il Ministero agisca quale Responsabile del trattamento, invece, nel Registro del Trattamento dovranno essere riportate, come minimo, le informazioni di seguito indicate:

- ✓ il nome e i dati di contatto:
  - o del Responsabile del trattamento;
  - o di ogni Titolare del trattamento per conto del quale agisce il Responsabile del trattamento;
  - o ove applicabile, del Rappresentante del Titolare del trattamento o del Responsabile del trattamento (qualora questi risiedano al di fuori dell'UE);
  - o del DPO;
  - o dell'Esercente le funzioni di Titolare al quale fa riferimento il trattamento affidato;
- ✓ le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
- ✓ ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del RGPD, la documentazione delle garanzie adeguate;
- ✓ ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1. 3.

4.5 GESTIONE DEGLI EVENTI DI VIOLAZIONE (DATA BREACH)

Per ottemperare ai requisiti normativi sulla rilevazione e il monitoraggio degli incidenti di sicurezza, il Ministero definirà un proprio modello di gestione volto a garantire la protezione dei Dati Personali per fronteggiare il verificarsi di eventi che potrebbero costituire una violazione dei Dati Personali.

A titolo esemplificativo e non esaustivo, gli eventi di possibile violazione dei Dati Personali possono essere costituiti da:

- ✓ distruzione di dati informatici o documenti cartacei (intesa come indisponibilità irreversibile di dati con accertata impossibilità di ripristino degli stessi), conseguente ad eliminazione logica (es. errata cancellazione dei dati nel corso di un intervento manuale o automatizzato) o fisica (es. rottura di dispositivi di memorizzazione informatica, incendio/allagamento locali dove sono archiviati i contratti ed altri documenti degli interessati);

- ✓ perdita di dati, conseguente a smarrimento/furto di supporti informatici (es. laptop, HD, supporti di memorizzazione rimuovibili) o di documentazione contrattuale o altri documenti cartacei (in originale o in copia);
- ✓ accesso non autorizzato o intrusione nei sistemi informatici tramite lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione oppure attraverso la compromissione o rilevazione abusiva di credenziali di autenticazione (es. user id e password) per l'accesso ai sistemi;
- ✓ modifica non autorizzata di dati, derivante ad esempio da un'erronea esecuzione di attività automatizzata sui sistemi informatici (aggiornamenti periodici) o da mettere in relazione ad un intervento umano;
- ✓ rivelazione di dati e documenti a soggetti terzi non legittimati, anche non identificati, conseguenti ad esempio alla fornitura di informazioni, anche verbali, a persone diverse dal soggetto legittimato (in assenza di delega formale di quest'ultimo), o altri documenti di valore contrattuale o esecutivo a soggetti diversi dall'effettivo destinatario o errata gestione di supporti informatici.

Qualsiasi episodio dal quale potrebbe discendere, anche solo potenzialmente, una violazione di dati personali deve essere segnalato e, eventualmente, sottoposto a opportuna escalation.

Le violazioni dei dati saranno poi oggetto di segnalazione telematica mediante l'apposito servizio disponibile sul sito del Garante della Protezione dei Dati Personali .

4.6 GESTIONE DEL RAPPORTO CON L'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nell'ottica di garantire l'efficacia del modello sviluppato e raggiungere i requisiti di compliance imposti dalla normativa sulla protezione dei dati personali, risulta necessario prevedere un processo di gestione dei rapporti con il Garante per la protezione dei dati personali che includa almeno:

- ✓ la consultazione preventiva (ex art. 36 del RGPD);
- ✓ il riscontro alle richieste del Garante;
- ✓ la notifica in caso di violazione dei Dati Personali.

I rapporti tra il Ministero e l'autorità Garante sono affidati, come previsto dall'art. 39 del RGPD, al RPD.

4.6.1 Consultazione preventiva

La consultazione preventiva è richiesta qualora la valutazione d'impatto sulla protezione dei dati, condotta ai sensi dell'art. 35 del RGPD, indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate.

La comunicazione trasmessa al Garante deve contenere almeno:

- ✓ responsabilità degli attori coinvolti nel Trattamento (Titolari, Contitolari, Responsabili, ecc.);
- ✓ le finalità e i mezzi del trattamento previsto;
- ✓ le misure e le garanzie previste per proteggere i diritti e le libertà degli Interessati;

- ✓ i risultati della valutazione d'impatto effettuata;
- ✓ ogni altra informazione che potrebbe essere utile per la valutazione da parte del Garante o da questi richiesta.

4.6.2 Riscontro alle richieste dell'Autorità garante per la protezione dei dati personali

L' Autorità garante per la protezione dei dati personali può richiedere informazioni relativamente a segnalazioni o ricorsi degli Interessati o, nell'ambito di indagini conoscitive, richiedere contributi informativi specifici; inoltre può, anche in occasione delle verifiche ispettive, raccogliere documentazione relativamente alle misure tecniche e organizzative implementate a protezione dei Dati Personali trattati, documentazione contrattuale, modelli e documenti privacy estendendo l'analisi a qualsiasi altro processo, misura o trattamento effettuato da parte del Titolare. Vi sono dei casi nei quali, viceversa, è il Ministero che può richiedere al Garante pareri e consultazioni su specifici argomenti ovvero per ambiti che necessitino di un'approvazione da parte dell'Autorità.

4.6.3 Notifica in caso di violazione dei dati personali

Con riferimento alle attività di notifica di violazione dei dati personali, di rimanda alla sezione 4.5 "Gestione degli eventi di Data Breach".

4.6.4 Ispezioni da parte dell'Autorità garante per la protezione dei dati personali

L' Autorità garante per la protezione dei dati personali (Garante) può effettuare ispezioni presso il Ministero finalizzate a verificare l'effettiva implementazione delle prescrizioni previste dalle normative applicabili.

Nel corso delle ispezioni svolte dal Garante, il Ministero adotterà le cautele ed i presidi previsti dalle proprie policy interne riguardanti i rapporti con autorità di pubblica vigilanza.

Il DPO ha il compito di interfacciarsi con i soggetti esterni in caso di ispezioni e dovrà gestire e coordinare la cooperazione tra il Garante e il Titolare.

Gli Autorizzati/Incaricati dovranno prestare la massima collaborazione ai funzionari del Garante che effettuino le suddette ispezioni e fornire tutte le informazioni attinenti alle operazioni di Trattamento di Dati Personali svolte che siano dagli stessi richieste.

4.7 FORMAZIONE ED INFORMAZIONE INTERNA

Gli interventi formativi sono finalizzati a rendere edotti gli Autorizzati/Incaricati del trattamento dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei Dati Personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal Titolare.

Il piano di formazione, gestito dall'Ufficio II - Contezioso, disciplina, formazione e controllo di gestione della Direzione generale del personale, del bilancio e dei servizi strumentali, viene erogato al personale già al

momento dell'ingresso in servizio e, nel seguito, periodicamente nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento di Dati Personali.

I moduli formativi avranno ad oggetto, in funzione dei relativi ambiti di competenza, i seguenti contenuti:

- ✓ finalità ed ambiti legislativi, adeguamento alla normativa ed ai Provvedimenti dell'Autorità Garante per la protezione dei dati personali;
- ✓ tipologia di dati e modalità di trattamento degli stessi;
- ✓ modello di gestione della protezione dei dati personali implementato;
- ✓ ruoli previsti per il trattamento dei dati personali;
- ✓ informativa e consenso, diritti di accesso, reclami e sanzioni;
- ✓ le misure di sicurezza adottate ed il ruolo di chi effettua i trattamenti nella loro corretta applicazione.

Inoltre, per garantire la diffusione delle conoscenze e della cultura in materia, tutta la documentazione relativa al Sistema di Gestione della protezione dei dati personali è resa disponibile a tutto il personale del Ministero mediante condivisione in apposita cartella della intranet ovvero con forme equivalenti.

4.8 SISTEMA DISCIPLINARE

Fermo quanto sopra descritto nella sezione 2.2 "Sistema Sanzionatorio" del presente documento, in relazione alla responsabilità degli Autorizzati/Incaricati, l'inosservanza degli obblighi previsti dal presente documento può assumere rilevanza disciplinare nei casi previsti dalle norme di legge e dai contratti con applicazione delle conseguenti sanzioni da parte del competente ufficio su segnalazione del Direttore/Dirigente.

5 STRUMENTI PER IL MONITORAGGIO E CONTROLLO DEL SISTEMA

5.1 REGISTRAZIONI, DOCUMENTAZIONE E FLUSSI INFORMATIVI

Il Titolare del trattamento, in base agli obblighi di accountability di cui all'art. 5 par. 2 del RGPD, ed i Referenti interni del trattamento devono implementare un sistema di monitoraggio per garantire il controllo sistematico dell'adeguatezza, efficacia ed effettiva operatività del sistema privacy implementato rispetto alla normativa in materia di protezione dei dati personali.

Il sistema di monitoraggio, verifica e controllo è fondato su due livelli distinti di intervento:

- controllo di primo livello (c.d. "controllo di linea"), posto in essere dai soggetti ai quali la Direttiva del 8.01.2021 attribuisce le funzioni del Titolare ("Esercenti le funzioni di Titolare"), coadiuvati dai responsabili delle unità organizzative ("Autorizzati/Incaricati") e dai Referenti privacy nell'ambito delle ordinarie funzioni di coordinamento e gestione delle attività di propria competenza;
- controllo di secondo livello (c.d. "controllo di compliance") affidato al RPD come descritto nell'apposito paragrafo del presente documento.

Gli specifici strumenti messi a disposizione di tali soggetti sono i seguenti:

a) **Registro delle Violazioni - Data Breach**: il registro consente la registrazione e tracciamento degli eventi (anche non sfociati in un incidente), degli incidenti e quasi-incidenti (situazioni anomale o incidenti di sicurezza) nonché delle vere e proprie violazioni - data breach, a prescindere se l'evento abbia dato luogo alla notifica al Garante e/o alla comunicazione agli interessati di cui agli artt. 33 e 34. Così configurato, il Registro consente di identificare e circoscrivere (per "tipologia di eventi" ovvero per asset/trattamento) gli ambiti di criticità maggiormente impattanti – in termini organizzativi, operativi e di compliance - sull'organizzazione ed eventualmente sugli interessati, al fine di poter evidenziare i principali o più critici ambiti di intervento da gestire mediante azioni correttive;

b) **Registro delle richieste di esercizio dei diritti degli interessati:** anche in questo caso, oltre a costituire un fondamentale strumento documentale per tracciare e poter dimostrare la compliance sul punto, il Registro consente di individuare eventuali attività o modalità di trattamento considerate "critiche" dagli interessati.

La tenuta dei Registri è affidata al RPD e gestita dalla sua struttura di supporto, mentre l'alimentazione degli stessi è garantita dai flussi informativi appresso regolati.

Ulteriori documenti e dati di input ai fini del monitoraggio e controllo del sistema privacy possono essere i seguenti:

- rendicontazioni periodiche e/o finali dei progetti/servizi affidati all'esterno, mediante specifica previsione contrattuale in capo al Responsabile esterno ex art. 28 del RGPD di relazionare sul buon esito delle attività di trattamento secondo le istruzioni impartite;
- relazioni periodiche circa l'andamento delle attività di competenza degli amministratori di sistema;
- audit report e relazioni periodiche formalizzate dal RPD nel corso degli audit e verifiche di competenza;
- rilevazione dei dati e valorizzazione degli indicatori di anomalia di cui al paragrafo seguente e conseguente verifica dello scostamento rispetto ai valori obiettivo ivi definiti (da considerarsi quali "alert" ovvero indici di situazioni di rischio potenziale).

Per effetto dell'approvazione del presente documento sono istituiti i seguenti **flussi informativi in favore del RPD:**

PERIODICITA'	DESCRZIONE FLUSSO INFORMATIVO	RESPONSABILE FLUSSO
Ad evento	Copia della richiesta di informazioni da parte dell'Autorità di protezione dei dati personali o di altre Autorità, altre PA o Forze dell'Ordine aventi ad oggetto i dati personali nella titolarità del MUR	Ufficio di protocollo del Segretario Generale
Ad evento	Notifiche relative a sanzioni in ambito protezione dei dati personali	Ufficio di protocollo del Segretario Generale

Ad evento	Scheda della rilevazione di evento di sicurezza (vedi procedura data-breach)	Esercenti le funzioni di Titolare
Ad evento	Verbale relative ad evento di "Violazione" notificato all'Autorità garante per la protezione dei dati personali	Esercenti le funzioni di Titolare
In funzione della criticità segnalata/ complessità della richiesta	Segnalazioni o richieste di esercizio dei diritti da parte degli Interessati	Esercenti le funzioni di Titolare
Tempestiva	Copia delle relazioni / verbali redatti in sede di audit di I° livello che presentano criticità nella protezione dei dati personali	Esercenti le funzioni di Titolare
Tempestiva	In presenza di modifiche significative ai trattamenti o di nuovi trattamenti che presentano rischi elevati per i diritti e le libertà degli Interessati	Esercenti le funzioni di Titolare

5.2 INDICATORI DI ANOMALIA DEL SISTEMA PRIVACY

Il seguente sistema di indicatori è gestito dal RPD ed è alimentato mediante gli strumenti di registrazione ed i flussi di cui al paragrafo precedente.

DIMENSIONE DEL MONITORAGGIO	DESCRIZIONE INDICATORE	VALORE SEGNALETICO	FONTE DI REPERIMENTO DEL DATO
COMPLIANCE ALLA NORMATIVA	Numero di richieste di esercizio dei diritti ex artt. 15 e ss. del RGPD o di reclami pervenuti dagli interessati nell'anno	> 10	Registro delle richieste di esercizio dei diritti
	Numero di richieste/reclami con identico oggetto o relative ad uno stesso trattamento	> 3	
	Tempi di risposta alle richieste di esercizio dei diritti da parte degli interessati	≥ 30 gg	
	Numero di ispezioni subite da pubbliche autorità su segnalazione/denuncia degli interessati nell'anno	> 1	Flussi informativi al RPD
	Numero di sanzioni comminate in materia da pubbliche autorità nell'anno	> 0	
	Numero di soggetti esterni che hanno rifiutato la designazione a Responsabile esterno del trattamento	> 2	

DIMENSIONE DEL MONITORAGGIO	DESCRIZIONE INDICATORE	VALORE SEGNALETICO	FONTE DI REPERIMENTO DEL DATO
CONTROLLO E MIGLIORAMENTO CONTINUO	Numero di privacy audit effettuati nell'anno	≤ 2	Verbali/relazioni di audit/ Relazioni agli Organi
	% di Non Conformità (NC) riscontrate (n. NC / n. audit)	≥ 30%	
	Numero relazioni del RPD agli Organi	< 2	Relazioni agli Organi

DIMENSIONE DEL MONITORAGGIO	DESCRIZIONE INDICATORE	VALORE SEGNALETICO	FONTE DI REPERIMENTO DEL DATO
SICUREZZA E DISPONIBILITÀ DEI DATI	Numero di segnalazioni di incidenti inserite nel Registro dei Data Breach	≥ 3/anno	Registro data breach
	Numero di violazioni di dati personali notificate al Garante Privacy ex art. 33 RGPD	> 1	
	Numero di data breach notificati al Garante oltre i termini previsti dal RGPD (72h)	> 1	
	Numero di violazioni di dati personali comunicate agli interessati ex art. 34 RGPD	> 1	
	Tempi medi di risoluzione incidenti e problematiche di sicurezza (sommatoria giorni tra segnalazione e risoluzione / numero segnalazioni)	≥ 7	Sistema ticketing interno / fornitori esterni
	Tempi medi di risoluzione incidenti bloccanti (sommatoria giorni tra segnalazione e risoluzione / numero segnalazioni)	≥ 2	

5.3 PRIVACY AUDIT

La realizzazione di verifiche e audit al fine di verificare l'applicazione della normativa e delle istruzioni impartite, ove necessario, è funzione affidata - nelle fasi di rilevazione dell'esigenza, programmazione e realizzazione – al RPD coadiuvato dalla struttura di supporto.

Le attività di verifica sono di regola programmate e previamente comunicate ai soggetti coinvolti (salvo esigenze di audit a sorpresa) e sempre condotte alla presenza degli stessi.

Gli esiti delle verifiche, formalizzati in forma di audit report, sono:

- condivise con i soggetti auditi che possono formalizzare chiarimenti e/o controdeduzioni,
- completate – in caso di rilevazione di Non conformità (NC) – dalla proposta di azioni correttive/preventive,
- formalizzate – immediatamente ove evidenzino NC, ovvero nell'ambito delle relazioni periodiche.

A seguito della conduzione degli audit, il RPD provvede ad alimentare gli indicatori di cui al paragrafo precedente.

6 RIESAME DEL SISTEMA DI GESTIONE DELLA PRIVACY

L'attuazione di un sistema di monitoraggio, verifica e controllo del sistema privacy implementato rispetto alla normativa e alle direttive e istruzioni impartite è una specifica responsabilità del Titolare del trattamento, rientrante negli obblighi di accountability di cui agli artt. 24 c 1 e 2 e 32 c 1 lett. d) del RGPD.

Nell'ottica del miglioramento continuo e del raggiungimento degli obiettivi di compliance alla normativa di riferimento, anche al fine di garantire che l'efficacia delle misure tecniche e organizzative implementate sia "testata regolarmente" (art. 32, par. 1, lett. d), del RGPD), il Sistema di gestione della Privacy delineato nel presente documento dovrà essere sottoposto a riesame, in occasione:

- dell'emanazione di nuove disposizioni normative, di pronunce giurisprudenziali, ovvero in relazione ad eventuali provvedimenti del Garante per la Protezione dei Dati di carattere cogente e/o interpretativo che abbiano un impatto sulla disciplina della protezione dei dati rilevante per il MUR;
- di cambiamenti significativi della struttura organizzativa o dei settori di attività del MUR che comportino la ridefinizione della governance interna, degli organigrammi e delle relative attività e responsabilità;
- in occasione dell'introduzione di nuovi significativi strumenti di gestione, rilevanti rispetto al trattamento di dati personali;
- nel caso di applicazione di sanzioni da parte dell'Autorità giudiziaria ovvero del Garante.

Il riesame è istruito con la collaborazione del RPD, il quale redigerà, ove richiesto, apposita relazione in merito, tenuto conto delle informazioni disponibili quali desunte dalle proprie attività di supporto e di controllo. L'eventuale relazione del RPD è trasmessa al Ministro, per il tramite del Segretario, per l'assunzione delle eventuali decisioni necessarie a garantire la compliance e il miglioramento continuo.

7 ACRONIMI E DEFINIZIONI

7.1 ACRONIMI

MUR	Ministero dell'Università e della Ricerca

MOP	Modello organizzativo privacy del MUR
RGPD	Regolamento Generale sulla Protezione dei dati Personali - General Data Protection Regulation (Regolamento UE 2016/679)
CODICE	Codice in materia di protezione dei dati personali (ex D. lgs. 196/2003 s.m.i)
EDPB e WP29	Comitato europeo per la protezione dei dati (European Data Protection Board) che ha sostituito il Working Party Article 29 (Gruppo di lavoro ex art. 29)
RPD/DPO	Responsabile della Protezione dei Dati del MUR

7.2 DEFINIZIONI

Amministratore di Sistema	Figura professionale/ruolo cui è demandata la gestione e/o la manutenzione di sistemi informatici e di elaborazione dati o di sue componenti sia hardware che software, come definiti dal Provvedimento Generale del Garante del 27 Novembre 2008 e s.m.i.
Autorità di controllo (Autorità)	Autorità di cui all'articolo 51 del Regolamento Europeo in materia di Protezione dei Dati Personali ovvero una o più Autorità pubbliche indipendenti incaricate da uno Stato Membro di sorvegliare l'applicazione del Regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali. In Italia l'Autorità di controllo indipendente è il Garante per la protezione dei dati personali (cd. "Garante Privacy").
Comunicazione	Dare conoscenza dei dati personali a uno o più soggetti diversi dall'interessato, dal rappresentante del Titolare o del Responsabile non stabiliti nel territorio dell'Unione europea, dalle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile o espressamente designate, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Valutazione d'Impatto - Data Protection Impact Assessment (DPIA)	Valutazione d'impatto sui Trattamenti dei Dati Personali che il Titolare effettua o prevede di effettuare, con lo scopo di verificare se il Trattamento presenti rischi elevati sui diritti e sulle libertà degli interessati.
Dati comuni (identificativi)	Dati attraverso i quali è possibile ottenere l'identificazione diretta dell'interessato.

	A titolo esemplificativo i codici identificativi, sia quelli ricavati da dati anagrafici (e.g. codice fiscale) sia i codici univoci attribuiti a una persona in base a criteri predefiniti (e.g. matricola), sono dati identificativi.
Dati giudiziari	Dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 RGPD).
Dati personali	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»), anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso 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.
Dati sensibili/particolari	Dati Personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Responsabile della protezione dei dati "RPD" **Data Protection Officer "DPO" (art. 37 e ss. del RGPD)**	Soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo. Coopera con l'Autorità e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali.
Diffusione	Dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Regolamento Generale sulla Protezione dei Dati personali (o RGPD) - General Data Protection Regulation (o "RGPD")	Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, che stabilisce la disciplina europea di regolamentazione in ambito di protezione dei dati personali.
Autorizzato/Incaricato	Persona fisica autorizzata a compiere operazioni di trattamento su dati personali per conto del Titolare.
Interessato	Persona fisica identificata o identificabile, direttamente o indirettamente, da un dato personale e comunque cui il dato trattato si riferisce.

Protezione dei dati fin dalla progettazione o per impostazione predefinita - Privacy by design e privacy by default	Misure tecniche e organizzative adeguate, messe in atto da Titolare, volte a garantire il rispetto dei principi relativi alla protezione dei dati personali sin dalla progettazione (privacy by design) e per impostazione predefinita (privacy by default).
Esercente le funzioni di Titolare del trattamento	Il soggetto al quale, con la Direttiva ministeriale adottata il 08.01.2021, il Ministro ha delegato l'esercizio delle funzioni del Titolare del trattamento per i rispettivi ambiti di competenza.
Referente privacy	Il soggetto individuato da parte di ciascun esercente le funzioni di Titolare per il presidio degli adempimenti rientranti nel proprio perimetro di attribuzione previsto dalla Direttiva ministeriale adottata il 08.01.2021.
Registro dei trattamenti	Strumento mantenuto dal Titolare e/o dal Responsabile del Trattamento che permette agli stessi di: ▪ tenere traccia delle operazioni di Trattamento effettuate all'interno della propria organizzazione; ▪ avere un documento/tool operativo di lavoro mediante il quale censire i dati trattati, le banche dati, i destinatari dei trasferimenti dei dati personali o che li possono trattare ed eventuali altri elementi rilevanti per la gestione dei dati personali; ▪ dimostrare di aver adempiuto alle prescrizioni del regolamento, nell'ottica del principio di "accountability".
Responsabile del Trattamento	Soggetto diverso da un dipendente o da un collaboratore e/o consulente al quale viene conferita la nomina a Responsabile in relazione ai trattamenti di dati personali effettuati per conto del Titolare sulla base di un contratto di servizio o collaborazione che definisce autonomamente, nel rispetto delle istruzioni ricevute, l'ambito delle attività, e delle relative responsabilità, delegate.
Titolare del trattamento (art. 4, n. 7 e art. 24 del RGPD)	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 ha inoltre il compito di assicurare l'implementazione delle misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio.
Trattamento	Qualunque operazione o complesso di operazioni, effettuati con o senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione,

	la cancellazione e la distruzione dei dati, anche se non registrati in una banca di dati.
Violazione dei dati personali (o Data Breach)	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.