TITOLARE DEL TRATTAMENTO

COMUNE di FIANO ROMANO
Città Metropolitana di Roma Capitale

MODELLO ORGANIZZATIVO PRIVACY

Manuale sulla Privacy

RIFERIMENTO NORMATIVO:

REGOLAMENTO (UE) 2016/679 - D.Lgs. 196/2003 ss.mm.ii.

Regolamento Generale sulla protezione dei dati

REALIZZAZIONE:

FONDAZIONE LOGOS P.A. (DPO/RPD)

Rev.	DATA	REALIZZAZIONE	VERIFICA	APPROVAZIONE
01	24/10/2025	FONDAZIONE LOGOS P.A.	SEGRETERIA GENERALE	TITOLARE DEL TRATTAMENTO

INDICE

1. INTRODUZIONE

1.1 DATI IDENTIFICATIVI DELL'ENTE

Nome Azienda / Ragione sociale	**Comune di Fiano Romano**
Legale rappresentante	**Sindaco Pro Tempore**
Sede legale / Operativa	Piazza Giacomo Matteotti n. 2, 00065 (RM)
Attività	**Ente Locale Rappresentativo**
Numero di telefono	(+39) 0765.4071
Indirizzo e-mail	PEO: info@comune.fianoromano.rm.it PEC: protocollo@pec.comune.fianoromano.rm.it
Cod. Fisc. /P.IVA	**C.F.** 01460220583 **P.IVA** 00997991005

1.2 DESCRIZIONE DELL'ATTIVITÀ

Il **Comune di Fiano Romano** è un Ente Locale autonomo, rappresentativo della propria comunità, ne cura gli interessi e ne promuove lo sviluppo, con autonomia statutaria, normativa, organizzativa e amministrativa, nonché autonomia impositiva e finanziaria nell'ambito dei propri statuti e regolamenti e delle leggi di coordinamento della finanza pubblica. Il Comune è titolare di funzioni proprie e di quelle conferitegli con legge dello Stato e della Regione Lazio, secondo il principio di sussidiarietà. Le funzioni ad esso attribuite possono essere adeguatamente esercitate dalla autonoma iniziativa dei cittadini e delle loro formazioni sociali. Le specifiche funzioni sono, inoltre, definite dal Titolo II, Capo I del D.Lgs. n. 267/2000 (T.U.E.L.).

Il Comune di Fiano Romano si è dotato, ai sensi dell'art. 6 del T.U.E.L., di uno Statuto Comunale, adottato con Delibera del Consiglio Comunale n. 2 del 01/02/2001 e mod. con Delibera del Consiglio Comunale n. 48 del 04/07/2011.

Secondo l'art. 2 dello Statuto il "*Comune promuove lo sviluppo ed il progresso civile, sociale ed economico della propria comunità ispirandosi ai valori ed agli obiettivi della costituzione*", nonché "*persegue la collaborazione e la cooperazione con tutti i soggetti pubblici e privati e promuove la partecipazione dei cittadini, delle forze sociali, economiche e sindacali dell'amministrazione*", ispirando la propria azione al "*superamento degli squilibri economici, sociali e territoriali esistenti nel proprio ambito e nella comunità nazionale*" e alla "*promozione della funzione sociale dell'iniziativa economica, pubblica e privata, anche attraverso lo sviluppo di forme di associazionismo economico e di cooperazione*", asseverando il "*sostegno della realizzazione di un sistema globale ed integrato di sicurezza sociale e di tutela attiva della persona anche con l'attività delle organizzazioni di volontariato*" e, inoltre, tutelando e impegnandosi a sviluppare le "*risorse naturali, ambientali, storiche e culturali presenti nel proprio territorio per garantire alla collettività una migliore qualità della vita*".

1.3 ORGANIGRAMMA PRIVACY

Il Rappresentante del Titolare è il Sindaco Pro Tempore, o facente funzione di.

Il Titolare ha nominato un **Responsabile per la Protezione dei Dati Personali (DPO)** esterno, con Determinazione del Responsabile del Servizio n. 158 del 04.10.2022, la Fondazione Logos P.A. e nominato il personale Designato e Autorizzato come previsto ai sensi dell'art. 2-quaterdecies del D.Lgs. n. 196/2003 c.d. Codice Privacy e art. 29 del Reg. (UE) 2016/679.

I **Designati** sono **nominati a mezzo specifico atto istituzionale.** I Designati provvederanno con atto proprio a disciplinare gli **Autorizzati** del trattamento. Quest'ultima competenza spetta in via esclusiva al Dirigente dell'Area organizzativa di appartenenza, salvo atto di delega da parte di questa figura apicale ad eventuali Elevate Qualificazioni, o equiparate, del potere di disciplinare con proprio atto gli autorizzati sottoposti gerarchicamente.

L' **Amministratore di Sistema** è nominato ***esternamente***.

Il Titolare del Trattamento ha individuato il **Referente Privacy** interno all'Ente nella figura del **Segretario Generale**.

1.4 SCOPO

Il presente documento intende offrire un quadro generale di riferimento nonché idonee istruzioni per l'applicazione delle disposizioni del Reg. (UE) 2016/679 del "*Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*" (Regolamento Generale sulla Protezione dei Dati – R.G.P.D./G.D.P.R.).

1.5 CAMPO DI APPLICAZIONE

L'applicabilità della presente procedura coinvolge tutte le risorse comunali identificabili come incaricati del trattamento e ai responsabili esterni - che effettuano operazioni di trattamento dei dati personali per conto dell'organizzazione.

2. LA NORMATIVA SULLA PRIVACY

2.1 DEFINIZIONI

Ai fini del **Regolamento Europeo n. 2016/679 (G.D.P.R. o R.G.P.D.)** s'intende per:

- «***Dato personale***»*: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di*

identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

- ***«Trattamento»**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.*
- ***«limitazione di trattamento»:** il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;*
- ***«profilazione»:** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;*
- ***«pseudonimizzazione»:** il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;*
- ***«archivio»:** qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;*
- ***«titolare del trattamento»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;*
- ***«responsabile del trattamento»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;*
- ***«destinatario»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il*

trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

- ***«terzo»:*** *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;*
- ***«consenso dell'interessato»:*** *qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;*
- ***«violazione dei dati personali»:*** *la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;*
- ***«dati genetici»:*** *i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;*
- ***«dati biometrici»:*** *i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;*
- ***«dati relativi alla salute»:*** *i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;*
- ***«stabilimento principale»:***
  - *per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;*
  - *con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;*

- ***«rappresentante»:*** *la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;*
- ***«impresa»:*** *la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;*
- ***«gruppo imprenditoriale»:*** *un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;*
- ***«norme vincolanti d'impresa»:*** *le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;*
- ***«autorità di controllo»:*** *l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;*
- ***«autorità di controllo interessata»:*** *un'autorità di controllo interessata dal trattamento di dati personali in quanto:*
  - *il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo*
  - *gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure*
  - *un reclamo è stato proposto a tale autorità di controllo;*
- **«*trattamento* transfrontaliero»**:
  - *trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure*
  - *trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;*
- ***«obiezione pertinente e motivata»:*** un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle

libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

- ***«servizio della società dell'informazione»:*** il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;
- ***«organizzazione internazionale»:*** un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

2.2 AUTORITÀ DI CONTROLLO (GARANTE)

Ogni Stato membro dell'Unione europea ha la sua Autorità di controllo che è competente per la gestione dei reclami ad essa proposti o per eventuali violazioni del regolamento europeo e delle norme nazionali in materia di protezione dei dati, ma solo se l'oggetto riguarda uno stabilimento nel territorio dello Stato membro o incide in modo sostanziale sugli interessati unicamente nel suo Stato membro.

Il Garante per la protezione dei dati personali (Garante Privacy) è l'autorità di controllo nazionale italiana, un'autorità amministrativa indipendente istituita dalla legge sulla privacy (**Legge 31 dicembre 1996, n. 675**), in attuazione della Direttiva comunitaria 95/46/CE. Oggi è disciplinata dal Codice in materia di protezione dei dati personali (**D. Lgs. 30 giugno 2003 n. 196**). La sua sede è a Piazza di Montecitorio n. 121 in Roma.

Il Garante si occupa di:

- verificare la conformità alla legge dei trattamenti e prescrivere ai titolari le misure da adottare;
- esaminare reclami e segnalazioni e decidere sui ricorsi;
- limitare, sospendere o vietare i trattamenti in violazione delle norme;
- adottare le autorizzazioni generali;
- promuovere codici di deontologia e buona condotta (es. in materia di giornalismo);
- partecipare alle attività comunitarie e internazionali (anche quale componente del Gruppo Articolo29).

L'autorità di controllo ha il potere di irrogare sanzioni. Essi consistono nel:

- rivolgere avvertimenti al titolare o al responsabile del trattamento sul fatto che i trattamenti previsti possono violare le norme;
- rivolgere ammonimenti al titolare o al responsabile del trattamento ove i trattamenti abbiano violato le norme;
- ingiungere al titolare o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i relativi diritti;
- ingiungere al titolare o al responsabile del trattamento di conformare i trattamenti alle norme, specificando eventualmente le modalità e i termini per la conformità;

- imporre una limitazione provvisoria o definitiva al trattamento, sospendere temporaneamente il trattamento, o vietare del tutto;
- ordinare la rettifica, la cancellazione o l'aggiornamento dei dati personali;
- revocare le certificazioni o ingiungere all'organismo di certificazione di ritirare le certificazioni rilasciate se i requisiti non sono soddisfatti;
- infliggere le sanzioni amministrative pecuniarie;
- ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

2.3 FRAMEWORK PER LA CYBERSICUREZZA

A seguito della pubblicazione in Gazzetta Europea del 27 dicembre 20220 L 333/80 della Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a "*misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)*" sono stati approvati in Italia la Legge n. 90 del 28 giugno 2024 **"***Disposizioni in materia di rafforzamento della cybersicurezza e di reati informatici***"**, G.U. del 2 luglio 2024 n. 153, ed il **Decreto Legislativo n. 138 del 4 settembre 2024** di "*Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148"* , G.U. del 1 ottobre 2024 n. 230.

I **soggetti destinatari** della Direttiva (UE) n. 2022/2555 NIS II, ai sensi dell'art. 2 e 3, sono:

- Fornitori di servizi di cui all'allegato I (*energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, acqua potabile, acque reflue, infrastrutture digitali, gestione dei servizi TIC b2b*) o II (*servizi postali e corriere, gestione dei rifiuti, fabbricazione e produzione sostanze chimiche, produzione e trasformazione e distribuzione di alimenti, fabbricazione di dispositivi, fornitori di servizi digitali, enti di ricerca*) qualora:
    - Forniscano reti di comunicazione elettronica pubblica o di servizi di comunicazione elettronica accessibile al pubblico; Registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio; Prestatori di servizi di fiduciari.
- Soggetto fornitore unico di un servizio essenziale per il mantenimento di attività sociali o economiche fondamentali in uno Stato membro;
- Soggetto critico in ragione della sua particolare importanza a livello nazionale o regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nello Stato membro;
- Enti della pubblica amministrazione come segue:
    - Dell'amministrazione centrale quale definito da uno Stato membro conformemente al diritto nazionale;

- A livello regionale quale definito da uno Stato membro conformemente e al diritto nazionale che, a seguito di una valutazione basata sul rischio, fornisce servizi la cui perturbazione potrebbe avere un impatto significativo su attività sociali o economiche critiche.

- Soggetti critici ai sensi della Direttiva (UE) 2022/2557 relativa alla resilienza dei soggetti critici , indipendentemente dalle loro dimensioni, identificati.

Il **D.Lgs. n. 138/2024** si applica:

1. Alle Pubbliche amministrazioni individuate sulla base di un criterio di gradualità, dell'eveoluzione del grado di esposizione al rischio della PA, della probabilità che si verifichino incidenti e della loro gravità; nonché
2. Indipendentemente dalle dimensioni (anche P.M.I.), a: **(i)** i soggetti che forniscono servizi di trasporto pubblico locale, **(ii)** gli istituti di istruzione che svolgono attività di ricerca**, (iii)** i soggetti che svolgono attività di interesse culturale, **(iv)** le società *in house*, società partecipate e società a controllo pubblico, come definite nel D.Lgs. 19 agosto 2016, n. 175 (Testo unico in materia di società a partecipazione pubblica).

Per l'elencazione completa si rimanda agli Allegati I, II, III e IV che ricomprende i settori altamente critici e critici, le categorie di pubbliche amministrazioni e le ulteriori tipologie di soggetti.

Dal 1° dicembre 2024 e non oltre il 28 febbraio 2025, i soggetti pubblici e privati a cui si applica la normativa devono registrarsi attraverso il portale messo a disposizione dall'**Agenzia per la Cybersicurezza Nazionale** (A.C.N.).

Per agevolare l'adeguamento sostenibile agli altri obblighi normativi, il decreto introduce il principio della graduale implementazione degli stessi. Prevede, in particolare, che i primi obblighi di base, per le notifiche di incidente e le misure di sicurezza, vengano definiti a valle delle consultazioni nell'ambito dei tavoli settoriali, con determine del Direttore Generale di A.C.N. da adottarsi entro il primo quadrimestre del 2025.

Per favorirne l'efficace attuazione, il decreto legislativo stabilisce una differenziata finestra temporale di implementazione: 9 mesi per le notifiche e 18 mesi per le misure di sicurezza, decorrenti dalla data di consolidamento dell'elenco dei soggetti N.I.S. (articoli 31 e 40), decorrenti dalla data di consolidamento dell'elenco dei soggetti N.I.S. (aprile 2025).

Nell'impianto regolatorio è di fondamentale importanza anche il principio di proporzionalità, realizzato tramite l'attività di categorizzazione delle attività e dei servizi dei soggetti N.I.S. (articolo 30). L'attività, che dovrà essere condotta a partire dal 2026 (articolo 42), consentirà ai soggetti NIS di distinguere, all'interno della loro organizzazione e con il supporto di A.C.N., i diversi livelli di esposizione al rischio dei propri sistemi informativi e di rete.

A tali sistemi si applicheranno, coerentemente con la loro esposizione al rischio, maggiori obblighi finalizzati a innalzarne maggiori obblighi finalizzati a innalzare progressivamente i livelli di sicurezza informatica.

3. DISPOSIZIONI OPERATIVE

3.1 INFORMATIVA E CONSENSO

L'informativa è dovuta ogni qual volta vi sia un trattamento di dati. È una comunicazione rivolta all'interessato finalizzata ad informarlo sulle finalità e le modalità del trattamento dei dati operato dal titolare del trattamento ed anche a permettere che l'interessato possa rendere un valido consenso, quando sia necessario.

I contenuti dell'informativa sono elencati negli articoli 13, paragrafo 1, e 14, paragrafo 1 del Regolamento Europeo 2016/679. In particolare, il titolare deve sempre specificare i dati di contatto propri e del RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer) ove esistente, la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti. I fondamenti di liceità del trattamento sono indicati all´art. 6 del regolamento e sono: consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Il titolare deve anche specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo. Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione.

Il regolamento specifica che l'informativa deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice, soprattutto quando l'informativa sia rivolta ai minori.

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online).

Il consenso dell'interessato al trattamento dei dati personali dovrà essere preventivo e inequivocabile, anche quando espresso attraverso mezzi elettronici (ad esempio, selezionando un'apposita casella in un sito web). Per trattare i dati "particolari" (art. 9 del Regolamento Europeo 2016/679) il Regolamento prevede che il consenso debba essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su

trattamenti automatizzati (compresa la profilazione - art. 22). Infatti, se il trattamento è finalizzato ad attività di marketing diretto, l'interessato ha sempre il diritto di opporsi alla profilazione. Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate.

Il consenso potrà essere revocato in ogni momento. Il consenso si ritiene nullo nel caso di oggetto di scambio come nel caso di accesso a servizi on line o di scontista applicata in cambio del consenso (in quanto non si considera più libero). I trattamenti effettuati fino a quel momento dal titolare sulla base del consenso rimarranno comunque legittimi.

L'informativa diventa sempre di più uno strumento di trasparenza riguardo al trattamento dei dati personali e all'esercizio dei diritti. Per facilitare la comprensione dei contenuti, nell'informativa si potrà fare ricorso anche a icone, identiche in tutta l'Unione europea.

L'informativa è un atto unilaterale e in generale non è necessario che venga controfirmata, ma sarebbe comunque opportuno avere l'evidenza della sua avvenuta consegna (conservazione dell'e-mail di invio o firma per ricevuta consegna da parte del dipendente).

3.1 RACCOMANDAZIONI DELL'AUTORITÀ GARANTE SULL'INFORMATIVA

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

fermo restando che il GDPR supporta chiaramente il concetto di informativa "*stratificata*", più volte esplicitato dal Garante nei suoi provvedimenti in particolare attraverso l'impiego di icone associate (in vario modo) a contenuti più estesi, che devono essere facilmente accessibili, e promuove l'utilizzo di strumenti elettronici per garantire la massima diffusione e semplificare la prestazione delle informative, una volta adeguata l'informativa nei termini sopra indicati, i titolari potranno continuare o iniziare a utilizzare queste modalità per la prestazione dell' informativa, comprese le icone che l'Autorità ha in questi anni suggerito nei suoi provvedimenti (videosorveglianza, banche, ecc.) – in attesa della definizione di icone standardizzate da parte della Commissione vanno adottate anche le misure organizzative interne idonee a garantire il rispetto della tempistica:

il termine di 1 mese per l'informativa all'interessato è chiaramente un termine massimo, e occorre ricordare che l'art. 14, paragrafo 3, lettera a) del Regolamento Europeo 2016/679menziona in primo luogo che il termine deve essere "*ragionevole*" poiché spetta al titolare valutare lo sforzo sproporzionato richiesto dall'informare una pluralità di interessati, qualora i dati non siano stati raccolti presso questi ultimi, e salva l'esistenza di specifiche disposizioni normative nei termini di cui all'art. 23, paragrafo 1, del Regolamento Europeo 2016/679, è utile fare riferimento ai criteri evidenziati nei provvedimenti con cui il Garante ha riconosciuto negli anni l 'esistenza di tale sproporzione.

3.2 GESTIONE DELLA DOCUMENTAZIONE

In riferimento alla sicurezza e riservatezza dei dati personali conservati negli archivi aziendali, il Titolare del Trattamento, **Comune di Fiano Romano,** si è impegnato ad adottare le seguenti regole e procedure che il personale autorizzato del trattamento deve osservare. In particolare, l'accesso agli archivi cartacei da parte del personale autorizzato è limitata ai soli dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;

La chiave degli archivi è fornita solo al personale autorizzato è presente un Registro degli accessi che traccia le entrate e le uscite. Tutta la documentazione contenente dati particolari di cui all'art. 9 del GDPR viene conservata all'interno di fascicoli o supporti cartacei in armadi muniti di serratura con chiave che devono essere chiusi al termine della giornata di lavoro (come da istruzioni fornite al personale autorizzato).

Sono previsti dispositivi di sicurezza passiva (rilevatori di fumo, allarme, estintori).

In riferimento alla sicurezza nella cancellazione dei dati, il **Comune di Fiano Romano**, ha adottato le seguenti regole che gli incaricati del trattamento hanno l'obbligo di:

- La cancellazione dei dati può essere effettuata quando la conservazione degli stessi non risulta più essere necessaria ai fini per cui sono stati raccolti e successivamente trattati;
- I dati possono essere cancellati anche su richiesta dell'interessato, sempre che la conservazione non sia necessaria per legge;
- La distruzione dei dati avviene con sistemi meccanici o automatizzati in modo da evitare ogni possibile recupero.

3.2.1 DISPOSIZIONI SPECIFICHE IN CASO DI CESSAZIONE O CAMBIAMENTI ORGANIZZATIVI DEL RAPPORTO LAVORATIVO

In caso di cessazione del rapporto lavorativo o di cambiamenti organizzativi, ivi inclusi il trasferimento in comando e in distacco presso altra amministrazione o ente di natura pubblica (cfr. sub 3.10.2), il Titolare del Trattamento, attraverso appositi atti di gestione e conservazione documentale, anche informatica, nonché apposite policy informative, si impegna a:

- Richiedere al dipendente autorizzato di effettuare periodici back-up dei dati trattati, anche informatici, su appositi sistemi gestionali in uso presso l'Ente, escludendo, salvo speciali eventualità e previe apposite procedure di sicurezza (crittografia, pseudonimizzazione, etc.), l'utilizzo di supporti esterni, nonché di imporre la rigida separazione dei dati personali da quelli trattati in ambito lavorativo nei Dispositivi aziendali in uso al dipendente;
- Operare, contestualmente alla restituzione di eventuali Dispositivi aziendali in uso al dipendente, una procedura di formattazione degli stessi, al fine di eliminare eventuali dati personali non relativi alla posizione organizzativa ricoperta e alle mansioni attribuite;

- Per l'utilizzo di caselle di posta elettronica e di medi da parte dei dipendenti, il Titolare si impegna a fornire apposite caselle di posta istituzionale, con specifiche istruzioni e credenziali, per utilizzo esclusivo della corrispondenza in ambito lavorativo e atti correlati, escludendo qualsiasi tipo di corrispondenza personale. Al termine del trattamento lavorativo o a seguito di un cambiamento nelle mansioni del dipendente, il Titolare, per tramite del Responsabile dei sistemi informativi e/o dell'Amministratore di sistema, si impegna a sospendere detto account, reindirizzando il contenuto eventualmente ancora in arrivo a nuova casella per un periodo massimo di mesi tre (3), al termine del quale l'account e tutta la corrispondenza ivi contenuta, compresa la documentazione allegata, sarà cancellata definitivamente. Resta ferma la possibilità di conservare per necessità di difesa giudiziale, contenzioso e verifiche dell'Autorità Giudiziaria, il contenuto della casella di posta fino ad anni cinque (5), garantendo l'accesso esclusivo a tale contenuto a personale autorizzato per dette specifiche finalità, prorogabili per le specifiche e documentate esigenze del caso;
- La conservazione dei *log* di accesso e di corrispondenza, c.d. *metadati esteriori*, sarà conservata coerentemente con gli indirizzi più recenti del Garante per la Protezione dei Dati personali e con le politiche del provider del servizio di posta elettronica, salvo specifiche necessità di sicurezza informatica e dettami dell'Autorità per la Cybersicurezza Nazionale.

3.2.2 DISPOSIZIONI SPECIFICHE PER L'UTILIZZO DI DISPOSITIVI IN SMART WORKING O LAVORO AGILE

Fermo restando quanto previsto dalle policy del Titolare del Trattamento e nell'eventuale Disciplinare dei Sistemi Informativi, si definisce il **lavoro agile o "*smart working*"** come quella particolare **modalità di esecuzione della prestazione** di lavoro subordinato introdotta al fine di incrementare la competitività e di agevolare la conciliazione dei tempi di vita e lavoro.

La disciplina di riferimento è la Legge 22 maggio 2017, n. 81 come da ultimo modificata dalla Legge 4 agosto 2022, n. 122 (che ha convertito con modificazioni il D.L. 21 giugno 2022, n. 73, c.d. Decreto Semplificazioni), secondo la quale il lavoro agile è una modalità di esecuzione del rapporto di lavoro subordinato stabilita mediante **accordo tra le parti**, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa. La prestazione lavorativa viene eseguita in parte all'interno dei locali aziendali e in parte all'esterno, senza una postazione fissa, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale derivanti dalla legge e dalla contrattazione collettiva (art. 18, comma 1).

Il lavoratore è consapevole che lo *Smart Working* comporta lo svolgimento dell'attività lavorativa al di fuori della sede di lavoro e, pertanto, in condizioni che sono potenzialmente più esposte al rischio correlato alla compromissione della confidenzialità e della riservatezza delle informazioni aziendali.

Anche in considerazione di ciò, il lavoratore che svolge la propria attività in modalità agile è tenuto a custodire con diligenza e massima riservatezza tutte le informazioni aziendali ricevute ed è tenuto a comportarsi in maniera che la riservatezza e la confidenzialità delle informazioni aziendali sia mantenuta.
Gli utilizzatori dei dispositivi a supporto dello *smart working* devono rispettare le seguenti regole di condotta:

- Nel caso di dispositivi propri, è necessario creare un profilo utente separato sul proprio O.S. con credenziali distinte e non condivise in ambito familiare, custodendoli in maniera appropriata;
- Nel caso di dispositivi aziendali o comunque forniti dall'amministrazione, è necessario utilizzare il dispositivo fornito ed esclusivamente detto dispositivo, con l'utilizzo dell'account predisposto dal gestore della risorsa, per le finalità lavorative per il quale è stato assegnato; è categoricamente fatto divieto di creazione di ulteriori profili utenti, se non su specifica e motivata autorizzazione della struttura di appartenenza; è fatto, infine divieto di condivisione delle credenziali anche in ambito familiare;
- I dati trattati durante l'attività lavorativa devono essere accessibili unicamente all'utente in base al profilo autorizzativo di appartenenza e alle istruzioni impartite dal Titolare del Trattamento;
- È necessario configurare il blocco automatico dell'accesso al sistema dopo un breve periodo di inattività o bloccare manualmente l'accesso al sistema quando il dispositivo non è in uso;
- L'utilizzo di dispositivi removibili (*pen drive, hard disk esterni, etc.*) che prevedano sistemi di criptazione (*ad esempio, bitlocker, veracryptc, etc.*) sono ammessi solamente laddove preventivamente autorizzati e per specifiche finalità;
- È necessario effettuare il *logout* dai servizi web, dagli applicativi, Virtual Private Network e piattaforme di lavoro una volta terminata la sessione lavorativa, eseguendo periodicamente il *backup* dei dati secondo le istruzioni fornite dal Titolare del Trattamento;
- È necessario non introdurre consapevolmente software malevoli sulla rete o sui dispositivi utilizzati in *smart working*, non collegandoli a reti e Virtual Private Network sconosciute, ovvero prestando attenzione ad allegati e e-mail contenenti collegamenti sconosciuti che potrebbero portare ad attività illecite e furti di dati;
- È necessario non utilizzare strumenti o tecniche che possano arrecare danni alle sottoreti o agli utenti dell'Ente (*ad esempio Port Scanner, Security Scanner, Network monitoring, honeypot, Denial of Service, etc.*);
- È necessario custodire adeguatamente le credenziali e non condividerle con terzi.

3.3 REGISTRO DEI TRATTAMENTI

Sono esentate dall'obbligo di tenuta del registro le imprese o le organizzazioni con meno di 250 dipendenti, a meno che il trattamento effettuato:

- possa presentare un rischio per i diritti e le libertà degli interessati,
- non sia occasionale,
- includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10 (cioè dati sensibili o giudiziari).

Qualsiasi azienda tratta dati particolari se ha dipendenti (ad esempio, un'aspettativa per motivi di salute o la scelta delle festività comandate), come del resto i liberi professionisti trattano dati personali altrui in maniera non occasionale.

Tenuto conto di tali precisazioni, l'organizzazione ha redatto i Registri dei Trattamenti resisi necessari all'adempimento degli obblighi di legge, i cui contenuti sono indicati all'art. 30 del Regolamento, fermo restando che il Titolare o il Responsabile può inserire ulteriori informazioni se lo ritiene opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti. Tali registri devono essere tenuti costantemente aggiornati e possono avere forma cartacea o elettronica.

3.4 TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento (o data controller) è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*" (art. 4. par. 1, n. 7 Regolamento Europeo 2016/679). Il titolare del trattamento non è, quindi, chi gestisce i dati, ma chi decide il motivo e le modalità del trattamento.

Il Registro del Titolare del trattamento è uno strumento che consente di avere un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico - indispensabile per ogni eventuale successiva valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica.

3.5.1 REGISTRO DEL TITOLARE DEL TRATTAMENTO

L'organizzazione ha adottato un Registro su supporto digitale, in formato *.pdf, conforme al Regolamento Europeo. Tale documento viene periodicamente revisionato ed aggiornato.

3.5 CONTITOLARE DEL TRATTAMENTO

La protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esigono una chiara ripartizione delle responsabilità, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del

trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento (*joint controllers)*.

Nel caso si configurasse tale responsabilità l'accordo di contitolarità:

a. definisce le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento Europeo, con particolare riferimento all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del GDPR, fermo restando quanto eventualmente stabilito dalla normativa specificatamente applicabile;
b. può designare un punto di contatto per gli interessati;
c. riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati.

Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato, ai fini dell'esercizio dei diritti previsti dagli articoli 15 e ss. del GDPR. Indipendentemente dalle disposizioni di tale accordo, l'interessato può esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento.

3.6 RESPONSABILE DEL TRATTAMENTO

Il Responsabile del trattamento (o data processor) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 Regolamento Europeo 2016/679).

Il ruolo del responsabile del trattamento di cui al regolamento europeo è chiaramente riservato ad un soggetto esterno all'azienda, con riferimento ai fornitori di servizi. Infatti, vi è uno specifico obbligo di predisporre un contratto per la designazione delle responsabilità a carico del responsabile.

3.7.1 REGISTRO DEL RESPONSABILE DEL TRATTAMENTO

Il **Comune di Fiano Romano,** qualora nominata in qualità di Responsabile del trattamento, redige e tiene aggiornato un apposito Registro del Responsabile del Trattamento, tenuto in forma telematica, in conformità all'art. 30 del G.D.P.R., all'interno del quale gli atti di nomina verranno archiviati e censiti.

3.7 CONTRATTO DI NOMINA DEI RESPONSABILI ESTERNI

In base all'art. 28 del nuovo regolamento generale europeo, la nomina del Responsabile del Trattamento deve avvenire tramite contratto o altro "*atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*".

In qualità di Titolare del Trattamento, l'organizzazione invierà il contratto di nomina, redatto in conformità all'art. 28 del Regolamento Europeo 2016/679, ad ogni nuovo fornitore o partner a cui conferirà dati personali e /o particolari sin dal primo rapporto commerciale.

I Responsabili esterni sono tutti i fornitori (aziende o liberi professionisti) che per conto dell'organizzazione trattino dati personali e / o particolari e giudiziari.

Un responsabile esterno non potrà avvalersi di un ulteriore responsabile senza la previa autorizzazione scritta (specifica o generale) del titolare del trattamento.

Il contratto giuridico dovrà quindi essere firmato da entrambe le parti (Titolare e Responsabile).

3.8 DESIGNATI AL TRATTAMENTO

L'Ente Titolare, ai sensi dell'art. 2 quaterdecies del D.Lgs. n. 196/2003 mm. D.lgs. n. 101/2018, procede a nominare i Dirigenti e le E.Q. delle Aree Organizzative o equiparate, nonché i Referenti Privacy delle rispettive aree, quali soggetti "*Designati al Trattamento*".

A tali soggetti verranno assegnate le seguenti funzioni:

- aggiornare il Registro dei trattamenti di cui all'art. 30 del Reg. UE n. 679/2016 e supportare il DPO ed il Referente Generale della Privacy, per tutti gli adempimenti previsti in materia di privacy;
- controllare che lo svolgimento delle attività all'interno del proprio settore avvenga secondo i principi generali contenuti nell'art. 5 del GDPR;
- individuare e autorizzare i propri collaboratori in qualità di "*autorizzati*" incaricati, in assenza di un provvedimento analogo dell'Amministratore Unico, che operano su ciascun trattamento, con il modello di nomina dell'autorizzato incaricato adottato dall'Ente, ma comunque idonee ad assicurare il rispetto del principio di accountability;
- verificare, che i contratti o altri atti giuridici che disciplinano i rapporti con i rispettivi "*Responsabili del Trattamento dei dati*" (cioè quei soggetti esterni all'Autorità che elaborano e trattano dati per conto del Titolare, generalmente fornitori di servizi) siano conformi a quanto previsto dall'art. 28 del GDPR;
- aggiornare la modulistica di propria competenza e le informative ai sensi degli artt. 13 e 14 relative da fornire agli interessati;
- segnalare al RPD/DPO, al Referente Privacy ed al Responsabile dei sistemi informativi e/o Amministratore di sistema i casi in cui si ritiene necessario/opportuno adottare ulteriori misure organizzative e tecniche a tutela dei dati trattati; ovvero l'esigenza di avviare preventivamente una valutazione d'impatto del trattamento.

3.8.1 REFERENTE GENERALE PRIVACY

Al facente funzione di Referente Privacy, il **Segretario Generale**, del **Comune di Fiano Romano** vengono assegnate le seguenti funzioni:

- coordinatore in materia di trattamento dei dati personali e tutela della riservatezza dei dati personali il gruppo di lavoro/Team Privacy;
- responsabile della verifica per il corretto svolgimento delle attività indicate dal Responsabile della Protezione dei dati personali (RPD) e fornite da parte del Titolare e dalle diverse figure coinvolte, in particolare:
    - pianificare azioni di *compliance* laddove si reputi opportuno coinvolgendo le varie figure di riferimento;
    - coinvolgere ed informare il RPD in ogni occasione ritenuta necessaria nell'ambito dell'attività di trattamento dei dati personali;
    - Verificare le Nomine dei vari Responsabili esterni ai sensi dell'art. 28 del Regolamento;
    - Verificare l'aggiornamento del Registro dei trattamenti ai sensi dell'art. 30 del Regolamento;
    - Verificare l'aggiornamento della modulistica/informative adottate;
    - Segnalare eventuali misure non ritenute corrette ai fini della tutela della privacy;
    - Aggiornare e conservare la documentazione del sistema di gestione della Privacy;
- punto di riferimento per ogni eventuale comunicazione con il RPD esterno individuato e nominato, salvo ulteriori referenti delegati internamente alla Struttura organizzativa della Segreteria, e con i vari referenti privacy individuabili degli altri settori;

Durante lo svolgimento di tale attività sarà supportato dalla consulenza del Responsabile della Protezione dei Dati personali (RPD/DPO).

3.9 RESPONSABILE PER LA TRANSIZIONE DIGITALE

Il **Responsabile per la Transizione al Digitale (RTD)**, responsabile dell'Ufficio per la Transizione Digitale (UTD) o assimilato, è una figura la cui nomina è obbligatoria per tutte le P.A., come previsto **dall'art. 17 del Codice dell'Amministrazione Digitale** (D.Lgs. n. 82/2005) e sollecitato dal Ministero per la Pubblica Amministrazione con la Circolare n. 3 del 1° ottobre 2018. È possibile ricorrere alla nomina di un RTD e di un UTD in forma associata. I compiti di un RTD e dell'UTD riguardano : coordinamento strategico dello sviluppo dei sistemi informativi di telecomunicazione e fonia; indirizzo e coordinamento dello sviluppo dei servizi, sia interni sia esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione; indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività; accesso dei soggetti disabili agli strumenti informatici e promozione

dell'accessibilità; analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa; cooperazione alla revisione della riorganizzazione dell'amministrazione; indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia; progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi; promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie; pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione, al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale.

Nello specifico dell'Organizzazione del Titolare del Trattamento l'Ufficio per la Transizione Digitale si occupa dell'amministrazione della rete locale e dei server comunali, l'acquisto e aggiornamento hardware e software, lo sviluppo di applicativi software, la gestione tecnica del sito comunale, la configurazione della posta elettronica dei dipendenti e degli uffici comunali; l'inventario dei beni informatici; l'acquisto di consumabili per stampanti e dispositivi di archiviazione dei dati; l'estrazione di dati particolari dall'archivio informatico per uffici o altri enti ; il supporto tecnico agli uffici per le procedure software ; la manutenzione hardware.

È possibile che l'Ente determini l'affidamento di un servizio di Supporto al Responsabile per la Transizione Digitale mediante trattativa diretta e adeguato atto di nomina a Responsabile del Trattamento ai sensi dell'art. 28 del Reg. (UE) 2016/679 per le prestazioni di :

1) Supporto alla *governance* complessiva;
2) Formazione di primo livello (livello base per tutti i dipendenti) e di livello specialistico per la progressiva acquisizione delle necessarie competenze digitali da parte degli Amministratori, del RTD, dei Dirigenti /PO e di tutti i dipendenti;
3) Attività di consulenza, con possibilità di inoltrare quesiti.

3.10 AUTORIZZATI AL TRATTAMENTO

Il Regolamento europeo non prevede espressamente la figura dell'incaricato, ma non ne esclude la nomina, facendo riferimento a persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile (art. 4, n. 10 Regolamento Europeo 2016/679).

Incaricato o autorizzato, di fatto è il soggetto, persona fisica, che effettua materialmente le operazioni di trattamento sui dati personali. Deve essere debitamente formato ed edotto sugli obblighi inerenti le misure di sicurezza.

3.10.1 INDICAZIONI COMPORTAMENTALI PER I SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI

Il Comune di Fiano Romano ha adottato il "Codice di Comportamento dei Dipendenti" con Deliberazione della Giunta Comunale n. 201 del 20.12.2013 quale strumento di prevenzione e atto a promuovere comportamenti di buona amministrazione, ispirati a principi di legalità, eticità e trasparenza. Il Titolare ha inoltre adottato, con D.G.P. n. 9 del 27.12.2024, il "Codice di Comportamento Aziendale", in conformità alle Linee Guida in materia di Codici di comportamento delle Amministrazioni pubbliche" Delibera A.N.A.C. n. 177 del 19.02.2020. Ai sensi del predetto, agli Artt. 14 – 16, ha disposto specifiche policies, con integrazioni e specificazioni rispetto al D.P.R. n. 62/2013 come mod. da D.P.R. n. 81/2023, per i comportamenti in servizio, per l'utilizzo di tecnologie informatiche, per l'utilizzo dei mezzi di informazione e dei *social media*; nonché ha ulteriormente determinato i rapporti con gli organi di informazione e la gestione delle risorse in dotazione.

Fermo restando gli atti già adottati, il Titolare del Trattamento impartisce specifiche istruzioni per il trattamento dei dati personali al personale dipendente autorizzato.

La designazione degli autorizzati può avvenire anche con unico atto per più persone. L'eventuale designazione non necessita di firma per accettazione, anche se è utile una presa visione quale prova della conoscenza dell'incarico. La normativa non prevede requisiti quantitativi per essere considerati autorizzati, per cui anche la semplice presa visione di un dato personale si qualifica come trattamento. L'organizzazione adotta un modello di verbale di nomina i cui si specificano, per ciascun soggetto, i trattamenti e gli archivi a cui ha accesso in qualità di incaricato. In particolare, il modello specificherà i trattamenti di dati personali cui il soggetto è autorizzato, le modalità di gestione dei dispositivi elettronici, computer, telefoni aziendali e portali; inoltre, fornirà raccomandazioni ulteriori in tema di sicurezza digitale e istruzioni operative riguardo alle eventuali violazioni di dati personali (*data breach*). Il documento verrà consegnato e dovrà essere firmato da tutti i lavoratori che, per conto del Titolare del Trattamento, gestiscano dati. Lo stesso dovrà essere periodicamente revisionato.

3.10.2 ASSEGNAZIONE TEMPORANEA DIPENDENTI IN COMANDO / IN DISTACCO

L'art. 56 del D.Lgs. n. 3/1957 "***Comando presso altra Amministrazione***" recita testualmente che «[*l*]*'impiegato può essere comandato a prestare servizio presso altra amministrazione statale o presso enti pubblici, esclusi quelli sottoposti alla vigilanza dell'amministrazione cui l'impiegato stesso appartiene. Il comando è disposto, per tempo determinato e in via eccezionale, per riconosciute esigenze*

di servizio o quando sia richiesta una speciale competenza. Al comando si provvede con decreto dei ministri competenti di concerto con il ministro per il Tesoro, sentiti l'impiegato ed il Consiglio di amministrazione. Per l'impiegato con qualifica non inferiore a Direttore Generale, si provvede con decreto del Presidente del Consiglio dei ministri, sentito il Consiglio dei ministri, su proposta dei ministri competenti di concerto con quello per il Tesoro. È vietata l'assegnazione anche temporanea di impiegati ad uffici diversi da quelli per i quali sono istituiti i ruoli cui essi appartengono». Il dipendente così comandato dovrà attenersi alle istruzioni ricevute e alle procedure dell'Amministrazione presso la quale è comandato, con apposito profilo autorizzativo laddove avrà accesso a banche dati, documenti, informazioni contenenti dati personali, fermo restando l'eccezionalità dell'istituto del comando, il mantenimento della medesima posizione giuridica e gli oneri di spesa a carico dell'Amministrazione di appartenenza, presso la quale il comandato mantiene il medesimo rapporto organico antecedente al provvedimento di comando. Nel caso di dipendente che si trovi a svolgere mansioni superiori a quelle originarie presso l'amministrazione ove è comandato, non ha diritto all'inquadramento nella qualifica superiore presso il proprio datore di lavoro, né al pagamento delle relative differenze retributive.

In caso di dipendente **distaccato**, l'impiegato dipendente viene assegnato ad un ufficio diverso da quello in cui è formalmente incardinato, ma comunque presso il medesimo Titolare del Trattamento, datore di lavoro, che conserva il potere direttivo che gli è proprio.

In caso di dipendente in **trasferta**, che comporta anch'essa una assegnazione meramente temporanea del dipendente ad una sede diversa da quella abituale (*Corte di Cassazione sent. n. 8004 del 14 agosto 1998)* è disposta nell'interesse e su disposizione unilaterale del Titolare del Trattamento datore di lavoro.

4. RESPONSABILIZZAZIONE DEL TITOLARE

L'art. 5 del regolamento europeo aggiunge il principio di responsabilizzazione (*accountability*) del titolare del trattamento. Il regolamento europeo, infatti, sposta il fulcro della normativa in materia di protezione dei dati personali dalla tutela dell'interessato e dei suoi diritti alla responsabilizzazione del titolare del trattamento.

Il titolare del trattamento, quindi, tenuto conto della natura, del contesto e della finalità del trattamento, dovrà garantire, ed essere in grado di dimostrarlo (appunto, renderne conto) che il trattamento è effettuato non solo in maniera conforme alla normativa, ma in maniera tale da non determinare rischi e quindi gravare sui diritti e le libertà degli interessati.

Leggendo l'articolo 25 si evince che l'approccio del Regolamento Europeo 2016/679 è centrato sulla protezione dei dati più che dell'utente medesimo. È un approccio basato sulla valutazione del rischio (*risk based approach*), con il quale si determina la misura di responsabilità del titolare o del responsabile del

trattamento, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti.

4.1 PRIVACY BY DESIGN E BY DEFAULT

Il Regolamento europeo per la protezione dei dati personali impone al titolare del trattamento l'adozione di misure tecniche ed organizzative adeguate al fine di tutelare i dati da trattamenti illeciti.

In particolare, introduce il principio di *privacy by design e privacy by default*, un approccio concettuale innovativo che impone alle aziende l'obbligo di avviare un progetto prevedendo, fin da subito, gli strumenti a tutela dei dati personali. Per definizione, il principio di *privacy by design* è volto a tutelare il dato protetto "sin dal momento della progettazione"; mentre il principio di *privacy by default* è volto a tutelare la vita privata per "impostazione predefinita".

Il concetto di *privacy by design* risale al 2010, già presente negli Usa e Canada. I principi che reggono il sistema sono i seguenti:

- prevenire non correggere;
- privacy come impostazione di default (*ad esempio*, non deve essere obbligatorio compilare un campo di un *form* il cui conferimento di dati è facoltativo);
- privacy incorporata nel progetto (come l'utilizzo di tecniche di pseudonimizzazione o minimizzazione dei dati);
- massima funzionalità, in maniera da rispettare tutte le esigenze (rifiutando le false dicotomie quali più *privacy* = meno sicurezza);
- sicurezza durante tutto il ciclo del prodotto o servizio;
- trasparenza;
- centralità dell'utente.

Il principio di *privacy by design* va definito come una ulteriore modalità di riduzione del trattamento ex ante, costituito dalla creazione di prodotti e servizi che tengano conto, sin dalla loro progettazione, delle regole e dei principi della protezione dei dati, in modo da minimizzare a priori non solo la raccolta dei dati ma anche i trattamenti successivamente effettuati.

Invece, il principio di *privacy by default* stabilisce che per impostazione predefinita le organizzazioni dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini.

Ne consegue che il titolare debba attuare specifiche misure che garantiscano un idoneo trattamento dei dati, che deve esser personalizzato, a seconda delle finalità e del tipo di operazioni da porre in essere. Tale obbligo varia a seconda della quantità dei dati personali raccolti, della portata del trattamento nonché del periodo di conservazione e dell'accessibilità.

4.1.1 ISTRUZIONI OPERATIVE PER BANDI DI GARA, CONTRATTI E CONVENZIONI

Con le presenti istruzioni il Titolare del Trattamento intende fornire delle Linee Guida operative per la corretta elaborazione di bandi di gara, contratti e convenzioni relativi ad erogazione di servizi e pianificazione degli stessi, conformemente alle prescrizioni di cui al Reg. (UE) n. 2016/679 e alla normativa in materia. Si intende quindi:

a. Fornire le indicazioni al Dirigente o Responsabile di riferimento per la predisposizione del servizio da appaltare, talché sia garantita l'immediata e chiara individuazione delle attività oggetto di appalto e di eventuali aspetti rilevanti ai sensi del G.D.P.R.;
b. Individuare, laddove detti documenti ed atti prevedano il trattamento di dati personali, anche indirettamente riconducibili, apposite "sezioni" o "clausole" da includere nei bandi, contratti, convenzioni e che costituiranno elementi essenziali degli stessi;
c. Consentire, in fase successiva alla redazione, la verifica da parte dell'Ufficio competente che l'oggetto di gara sia chiaramente identificato e che siano stati inseriti i contenuti necessari ai fini della normativa rilevante in tema di riservatezza;
d. Fornire le corrispondenti indicazioni nel caso di convenzioni e / o protocolli d'intesa che non prevedano per loro natura una procedura di gara.

Il processo per identificare le diverse categorie di rapporti stabiliti da un contratto o convenzione segue alcuni passi chiave, che includono:

1. **Descrizione del servizio richiesto.**
2. **Identificazione dei servizi oggetto dell'appalto.**
3. **Valutazione dell'applicazione del GDPR**, verificando il trattamento di dati personali.
4. **Classificazione dei servizi in base a una categoria predefinita**, considerando che un contratto può riguardare più categorie e richiedere diversi D.P.A. (*Data Protection Agreement* o Accordo di Protezione dei Dati).

Se il bando prevede la stipula di un contratto/convenzione, devono essere inseriti articoli che regolano ruoli e responsabilità in materia di protezione dati. In assenza di un successivo atto (es. finanziamenti per progetti), il D.P.A. deve essere incluso nel bando e compilato e firmato dal contraente, pena l'esclusione.
Il G.D.P.R. richiede obbligatoriamente un accordo tra le parti in caso di scambio o trattamento di dati personali. Per supportare la classificazione dei servizi, si utilizza una tabella con criteri distintivi per:

- Collocare i servizi in una o più categorie.
- Esplicitare le misure specifiche da includere nel documento finale.

In caso di dubbi o impossibilità di classificare un servizio, è necessario consultare il Referente Privacy o il Referente individuato del D.P.O.
Se un servizio comporta attività rilevanti ai sensi del G.D.P.R., è necessario includere nel disciplinare di gara, contratto o convenzione, prescrizioni specifiche suddivise in sezioni relative a:

- **Descrizione del servizio e verifica dell'ambito di applicazione del G.D.P.R.;**
- **Prescrizioni comportamentali per le risorse umane coinvolte;**
- **Prescrizioni per le risorse organizzative;**
- **Misure di sicurezza per le risorse tecnologiche.**

Le regolazioni devono considerare:

1. La **qualificazione del rapporto** con l'aggiudicatario secondo il G.D.P.R;
2. I contenuti da esplicitare nel bando e nel contratto successivo;
3. Prescrizioni specifiche per comportamenti, organizzazione e tecnologie.

Questi elementi sono definiti nei diversi **Data Protection Agreement (D.P.A)**:

- **D.P.A. Titolare-Responsabile** (o sub-responsabile) ai sensi dell'art. 28;
- **D.P.A. di Contitolarità** ai sensi dell'art. 26;
- **D.P.A. tra Titolari Autonomi** ai sensi delle Linee Guida dell'E.D.P.B. 2.0 del 7 luglio 2021.

In appalti o protocolli senza trattamento diretto di dati personali, ma con rischi di interferenza, il D.P.A. deve prevedere clausole per minimizzare e sanzionare eventuali incidenti. **Rischio di interferenza** significa accesso occasionale e non autorizzato ai dati personali, che va prevenuto attraverso istruzioni per evitare comportamenti che possano causare *Data Breach* o incidenti di sicurezza.

CAT.	DESCRIZIONE CATEGORIA	SERVIZI COMPRESI NELLA CATEGORIA	ELEMENTI DISTINTIVI AI SENSI DEL G.D.P.R.	ACCORDO DI PROTEZIONE DEI DATI PERSONALI
1	***Utilizzo di risorse umane, applicazioni e sistemi del contraente***	Servizi SaaS, Servizi Tesoreria, Conservazione a norma, Servizi che hanno una loro specifica regolazione.	Continuità del Servizio, disponibilità del Dato, evitare situazioni di *Lock In*.	Titolare/Responsabile Titolari autonomi
2	***Utilizzo sistemi IT e SW di base del contraente***	Servizi IaaS.	Continuità del servizio, individuazione dei trattamenti di Information Technology (IT).	Titolare/Responsabile (solo per i servizi di gestione IT) Titolari autonomi per specifici servizi (es. *posta elettronica, SPID, portali amministrativi in*

				rete)
3	***Servizio nel quale deve essere prevista la distruzione dei supporti magnetici e non, contenenti dati personali***	Rottamazione Hardware, Gestione archivi di deposito.	Garanzie sulla distruzione del supporto fisico, modalità di esecuzione (la distruzione del supporto fisico non significa la distruzione del dato che può continuare ad essere presente su altri supporti).	Titolare/Responsabile
4	***Servizi con uso prevalente di risorse umane che utilizzano per lo svolgimento delle proprie attività strumenti e mezzi di loro proprietà***	Servizi di assistenza tecnica su finanziamenti europei, servizi di help desk, portierato, consulenza, progettazione, vigilanza, somministrazione di lavoro, servizi di sorveglianza sanitaria, servizi di orientamento e formazione lavoratori in difficoltà, servizi di formazione del personale dell'ente, servizio di gestione sinistri- assistenza.	In questo caso l'elemento prevalente è l'utilizzo di risorse umane che svolgono il servizio, altrimenti ricadrebbe nella Cat. 1. Questa categoria si distingue dalla Cat. 5 in quanto le attività appaltate sono svolte con mezzi e strumenti di proprietà della ditta aggiudicatrice e non dell'ente. Per l'aggiudicatrice deve valutarsi la nomina a responsabile. Le misure di sicurezza varieranno tra Cat. 4 e Cat. 5.	Titolare/Responsabile Per i servizi legati all'esercizio di professioni regolate per legge, il rapporto è, di norma, fra Titolari autonomi (es. *servizi assicurativi, medico competente*)
5	***Servizi con uso***	Servizi di assistenza	Qualora il soggetto	Il rapporto è fra

	prevalente di risorse umane che utilizzano per lo svolgimento delle proprie attività strumenti e mezzi dell'ente.	tecnica su finanziamenti europei, servizi di help desk, portierato, stage, consulenza, progettazione, vigilanza, somministrazione di lavoro, produzione reportistica su conformità servizio web learning, servizi per l'impiego delle politiche attive.	contraente non abbia alcun controllo sulle modalità ed esecuzione delle attività di trattamento in quanto regolato da altre norme. Nel caso in cui si configuri una autonomia di mezzi e di strumenti in uso al contraente sarà in essere un rapporto titolare-responsabile.	titolari autonomi e il committente procede ad autorizzare il personale esterno. Titolare/Responsabile
6	***Servizi in relazione a progetti di interesse regionale cofinanziati/finanziati dalla Regione***	Contratti/convenzioni con soggetti terzi che svolgono servizi sul territorio con finanziamento / cofinanziamento regionale.	In questo caso si configura un rapporto tra titolari ed in capo alla Regione rimane il monitoraggio dei trattamenti	Titolarità autonoma
7	***Servizi nell'ambito dei mezzi di comunicazione di massa in rete e social***	Monitoraggio dei mezzi di comunicazione di massa in rete.	Se i servizi hanno ad oggetto soltanto dati pubblici non comportano trattamenti. Nel caso in cui per l'esercizio di tali attività fossero coinvolti dati personali dell'appaltatore si configura un rapporto di titolare	Nulla Titolare/ Responsabile Prescrizioni

			responsabile. Se esistessero rischi di diffusione o accesso indebito a dati personali debbono essere previste prescrizioni specifiche	
8	***Servizi di assistenza, manutenzione e sviluppo HW e SW***	Assistenza e manutenzione software e hardware, sviluppo e software	Attività di fornitura di servizi in ambito informatico (assistenza, manutenzione hardware e sviluppo software), che non prevedono trattamenti di dati personali, ma che potrebbero potenzialmente comportare accesso a dati personali da parte dell'esecutore. È necessario chiarire bene come si svolge l'attività e se in concreto potrà verificarsi un continuativo non occasionale accesso a contenitori di dati, in questo caso sarà necessario un rapporto titolare responsabile.	Prescrizioni Titolare/Responsabile

9	***Servizi nei quali l'attività appaltata è prettamente artigianale/manuale e l'utilizzo di mezzi e strumenti informatici non è prevalente***	Servizio mensa bar, manutenzione edifici ed impianti, pulizie, logistica.	Attività che per loro natura non comportano trattamento di dati, tuttavia, in alcuni casi (*es. nel servizio di pulizie, se il soggetto consulta dati erroneamente lasciati sulle scrivanie*) potrebbe esservi un coinvolgimento dell'aggiudicatrice e del suo personale in trattamenti, per cui devono essere indicate prescrizioni specifiche per tali ipotesi	Rapporto fra Titolari autonomi qualora siano coinvolti non in maniera occasionale dati personali Prescrizioni negli altri casi (*ad esempio accordi di riservatezza*)
10	***Servizi che vengono erogati congiuntamente fra più soggetti condividendo e individuando in modo congiunto le finalità, i mezzi e gli strumenti***	Sistema di prenotazioni fra aziende sanitarie diverse utilizzanti un unico sistema informativo. In questo caso si configura un rapporto fra titolari e se il servizio è dato in gestione ad un terzo, si configura un rapporto fra Contitolari e il Responsabile. Nel	Consuetudinariamente questa tipologia non si riscontra in appalti di servizi, bensì diviene possibile in convenzioni fra soggetti diversi che congiuntamente, condividendo finalità e mezzi, offrono un servizio comune per gli interessati e che pertanto li percepiscono come un soggetto unitario	In questo caso il rapporto fra i soggetti è di Contitolarità

		rapporto di contitolarità può essere identificato il soggetto Titolare che terrà i rapporti contrattuali e di altro tipo con il Responsabile.		
11	***Casi in cui l'aspetto del trattamento dati non sia previsto***	Servizio aereo con elicotteri di supporto al sistema regionale di prevenzione e lotta attiva agli incendi boschivi e di protezione civile, ovvero utilizzo di droni per finalità di pubblica sicurezza (*rilevanti ai fini della Dir. (UE) n. 680/2016*)	Casi in cui l'aspetto del trattamento dei dati non rileva.	Verificare se effettivamente non esistano rischi di accesso non strutturato a dati personali. Nel caso comunque fornire delle prescrizioni, verificando l'ambito di applicabilità del D.Lgs. n. 196/2003 e del D.Lgs. n. 51/2018

4.2 ANALISI DI SICUREZZA

L'organizzazione ha redatto il documento "Misure tecniche e organizzative ai sensi dell'art. 32 del regolamento europeo, atto a dimostrare l'adeguatezza delle misure di protezione fisica, implementate a tutela dei dati trattati. L'analisi delle misure tecniche ed organizzative mira a garantire la riservatezza, l'integrità e la disponibilità dei dati personali presenti nell'organizzazione.
Inoltre, a livello informatico viene aggiornata, da parte dell'Amministratore di sistema, periodicamente (almeno annualmente) la check list sulle misure minime di Sicurezza AGID.

L'organizzazione ha condotto per ogni trattamento un'analisi dei rischi secondo i principi espressi dall'E.N.I.S.A. (Agenzia Europea per la Sicurezza delle Reti e delle Informazioni), definendo prima il valore di impatto e di probabilità, con cui ricavare poi il livello rischio e le eventuali successive azioni correttive, che costituiscono il piano di miglioramento aziendale.

L'E.N.I.S.A. ha pubblicato un Manuale sulla sicurezza per il trattamento dei dati personali rivolto alle PMI (Piccole e Medie Imprese), fornendo un approccio pratico alla valutazione d'impatto, alla relativa analisi dei rischi e alle misure minime di sicurezza da gestire.

Le attività proposte sono strutturate in quattro step fondamentali:

1. una ricognizione del contesto e l'individuazione dei trattamenti compiuti;
2. una valutazione del potenziale impatto dei trattamenti compiuti sugli interessati;
3. una valutazione delle possibili minacce valutazione della loro probabilità di accadimento;
4. la valutazione del rischio (combinando la probabilità di accadimento della minaccia e l'impatto).

Seguendo la valutazione del rischio possono essere identificate le contromisure e i controlli suggeriti in base al livello di rischio valutato.

4.2.1 STEP 1: DEFINIZIONE DELL'OPERAZIONE DI TRATTAMENTO E DEL SUO CONTESTO

Il Titolare del trattamento deve definire i confini del sistema di trattamento dei dati oggetto di valutazione e *assessment* e del relativo contesto. Per supportare nella definizione dell'operazione di trattamento E.N.I.S.A. fornisce una serie di domande.

1. Cos'è l'operazione di trattamento dei dati personali?
2. Quali sono le tipologie di dati personali trattati?
3. Qual è la finalità del trattamento?
4. Quali sono gli strumenti utilizzati per il trattamento dei dati personali?
5. Dove avviene il trattamento dei dati personali?
6. Quali sono le categorie di soggetti interessate?
7. Chi sono i destinatari dei dati?

Rispondendo a queste domande, un'organizzazione deve considerare le varie fasi del trattamento dei dati (raccolta, conservazione, utilizzo, trasferimento, comunicazione, ecc.) e dei loro successivi parametri.

4.2.2 STEP 2: COMPRENSIONE E VALUTAZIONE DELL'IMPATTO

Il Titolare del trattamento in questa fase deve valutare l'impatto sui diritti e sulle libertà fondamentali delle persone fisiche derivanti dalla possibile perdita di sicurezza dei dati personali. Vengono considerati quattro livelli di impatto (Basso, Medio, Alto, Molto alto) come mostrato nella **Tabella 1** di seguito riportata.

VALORE	LIVELLO DI IMPATTO	DESCRIZIONE
1	**BASSO**	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
2	**MEDIO**	Gli individui possono andare incontro a significativi disagi, che saranno in

		grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
3	**ALTO**	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
4	**MOLTO ALTO**	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

***Tabella 1**: descrizione dei livelli di impatto*

La valutazione d'impatto è un processo qualitativo e il Titolare del Trattamento deve considerare una serie di fattori quali la tipologia di dati personali, la criticità dell'operazione di trattamento, il volume dei dati personali, le caratteristiche speciali del Titolare del trattamento, come anche le speciali categorie di interessati.

Per supportare il Titolare del trattamento in questo processo, la **Tabella 2** che segue può essere utilizzata per valutare separatamente l'impatto dalla perdita di riservatezza, integrità e disponibilità dei dati.

N.	DOMANDA	VALUTAZIONE
I.1.	Si prega di riflettere sull'impatto che una divulgazione non autorizzata (perdita di riservatezza) dei dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.	☐ Basso ☐ Medio ☐ Alto ☐ Molto alto
I.2.	Si prega di riflettere sull'impatto che un'alterazione non autorizzata (perdita di integrità) dei dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.	☐ Basso ☐ Medio ☐ Alto ☐ Molto alto
I.3.	Si prega di riflettere sull'impatto che una distruzione o perdita non autorizzata (perdita di disponibilità) di dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.	☐ Basso ☐ Medio ☐ Alto ☐ Molto alto

***Tabella 2**: domande di valutazione d'impatto*

Dopo questa valutazione, saranno ottenuti tre diversi livelli di impatto (per la perdita di riservatezza, integrità e disponibilità). Il più alto di questi livelli è considerato come il risultato della valutazione dell'impatto, relativo al trattamento complessivo dei dati personali.

4.2.3 STEP 3: DEFINIZIONE DI POSSIBILI MINACCE E VALUTAZIONE DELLA LORO PROBABILITÀ

Lo scopo del Titolare del trattamento è comprendere le minacce correlate al contesto complessivo del trattamento dei dati personali (esterno o interno) e valutare la loro probabilità (probabilità di accadimento della minaccia).

Per semplificare questo processo, sono state definite una serie di domande di valutazione che mirano a sensibilizzare le organizzazioni sull'ambiente di elaborazione dei dati (che è direttamente rilevante per le minacce). In tale prospettiva, le domande sono relative a quattro diverse aree di valutazione che interessano gli ambienti di elaborazione e trattamento dei dati, vale a dire:

- Risorse di rete e tecniche (hardware e software)
- Processi / procedure relativi all'operazione di trattamento dei dati
- Diverse parti e persone coinvolte nell'operazione di trattamento
- Settore di operatività e scala del trattamento

La **Tabella 3** riassume le domande relative alla valutazione della probabilità di occorrenza di una minaccia.

TIPO MISURA	DOMANDA	DESCRIZIONE
A. RISORSE DI RETE E TECNICHE	Qualche parte del trattamento dei dati personali viene eseguita tramite Internet?	Quando il trattamento dei dati personali viene eseguito in tutto o in parte tramite Internet, aumentano le possibili minacce da parte di aggressori esterni online (ad esempio Denial of Service, SQL injection, attacchi Man-in-the-Middle), soprattutto quando il servizio è disponibile (e, quindi, rintracciabile / noto) a tutti gli utenti di Internet.
A. RISORSE DI RETE E TECNICHE	È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)?	Quando l'accesso a un sistema di elaborazione interna dei dati viene fornito tramite Internet, la probabilità di minacce esterne aumenta (ad esempio a causa di aggressori esterni online). Allo stesso tempo aumenta anche la probabilità di abuso (accidentale o intenzionale) dei dati da parte degli utenti (ad esempio divulgazione accidentale di dati personali quando si lavora in spazi pubblici). Un'attenzione particolare dovrebbe essere prestata ai casi in cui è consentita la gestione / amministrazione remota del sistema IT.
A. RISORSE DI RETE E TECNICHE	Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	La connessione a sistemi IT esterni può introdurre ulteriori minacce dovute alle minacce (e ai potenziali difetti di sicurezza) inerenti a tali sistemi. Lo stesso vale anche per i sistemi interni, tenendo conto che, se non opportunamente configurati, tali connessioni possono consentire l'accesso (ai dati personali) a più persone all'interno dell'organizzazione (che in linea di principio non

TIPO MISURA	DOMANDA	DESCRIZIONE
		sono autorizzate a tale accesso).
A. RISORSE DI RETE E TECNICHE	Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	Sebbene l'attenzione sia stata posta su sistemi e servizi elettronici, l'ambiente fisico (rilevante per questi sistemi e servizi) è un aspetto importante che, se non adeguatamente salvaguardato, può seriamente compromettere la sicurezza (ad esempio consentendo alle parti non autorizzate di accedere fisicamente all'IT, apparecchiature e componenti di rete, o non riuscendo a fornire protezione della sala computer in caso di disastro fisico).
A. RISORSE DI RETE E TECNICHE	Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi?	Componenti hardware e software mal progettate, implementate e / o mantenute possono comportare gravi rischi per la sicurezza delle informazioni. A tal fine, le buone o le migliori pratiche accrescono l'esperienza di eventi precedenti e possono essere considerate come linee guida pratiche su come evitare esposizione (ai rischi) e raggiungere determinati livelli di resilienza.
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	Quando i ruoli e le responsabilità non sono chiaramente definiti, l'accesso (e l'ulteriore trattamento) dei dati personali può essere incontrollato, con conseguente uso non autorizzato delle risorse e compromissione della sicurezza complessiva del sistema.
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	Quando un uso accettabile delle risorse non è chiaramente obbligatorio, potrebbero sorgere minacce alla sicurezza a causa di incomprensioni o di un uso improprio, intenzionale del sistema. La chiara definizione delle politiche per le risorse di rete, di sistema e fisiche può ridurre i rischi potenziali.
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	I dipendenti che utilizzano i loro dispositivi personali all'interno dell'organizzazione potrebbero aumentare il rischio di perdita di dati o accesso non autorizzato al sistema informativo. Inoltre, poiché i dispositivi non sono controllati a livello centrale, possono introdurre nel sistema bug o virus aggiuntivi.
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	L'elaborazione di dati personali al di fuori dei locali dell'organizzazione può offrire molta flessibilità, ma allo stesso tempo introduce rischi aggiuntivi, sia legati alla trasmissione di informazioni attraverso canali di rete potenzialmente insicuri (es. Reti Wi-Fi aperte), sia uso non autorizzato di queste informazioni.
B. PROCESSI / PROCEDURE RELATIVI	Le attività di elaborazione dei dati personali possono	La mancanza di adeguati meccanismi di registrazione e monitoraggio può aumentare l'abuso intenzionale o accidentale di processi/ procedure e

TIPO MISURA	DOMANDA	DESCRIZIONE
ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	essere eseguite senza la creazione di file di registro?	risorse, con conseguente abuso di dati personali.
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	Quando l'accesso (e l'ulteriore trattamento) dei dati personali è aperto a un gran numero di dipendenti, le possibilità di abuso a causa del fattore umano incrementano. Definire chiaramente chi ha realmente bisogno di accedere ai dati e limitare l'accesso solo a quelle persone può contribuire alla sicurezza dei dati personali.
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	Quando l'elaborazione viene eseguita da contraenti esterni, l'organizzazione può perdere parzialmente il controllo su questi dati. Inoltre, possono essere introdotte ulteriori minacce alla sicurezza a causa delle minacce intrinseche a questi appaltatori. È importante che l'organizzazione selezioni gli appaltatori che possono offrire un massimo livello di sicurezza e definire chiaramente quale parte del processo è loro assegnata, mantenendo il più possibile un alto livello di controllo.
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	Quando i dipendenti non sono chiaramente informati sui loro obblighi, le minacce derivanti da un uso improprio accidentale (ad es. divulgazione o distruzione) di dati aumentano in modo significativo.
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	Quando i dipendenti non sono consapevoli della necessità di applicare le misure di sicurezza, possono causare accidentalmente ulteriori minacce al sistema. La formazione può contribuire notevolmente a sensibilizzare i dipendenti sia sui loro obblighi di protezione dei dati, sia sull'applicazione di specifiche misure di sicurezza.
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	Molte violazioni dei dati personali si verificano a causa della mancanza di misure di protezione fisica, come serrature e sistemi di distruzione sicura. I file cartacei sono solitamente parte dell'input o dell'output di un sistema informativo, possono contenere dati personali e devono anche essere protetti da divulgazione e riutilizzo non autorizzati.
D. SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO	Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	Quando gli attacchi alla sicurezza si sono già verificati in uno specifico settore dell'organizzazione del Titolare del trattamento, questa è un'indicazione che l'organizzazione probabilmente dovrebbe prendere ulteriori misure per evitare un evento simile.
D. SETTORE DI	La tua organizzazione	Se l'organizzazione è già stata attaccata o ci sono

TIPO MISURA	DOMANDA	DESCRIZIONE
OPERATIVITA' E SCALA DI TRATTAMENTO	ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	indicazioni che questo potrebbe essere stato il caso, è necessario prendere ulteriori misure per prevenire eventi simili in futuro.
D. SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO	Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	Bug di sicurezza / vulnerabilità possono essere sfruttati per eseguire attacchi (cyber o fisici) a sistemi e servizi. Si dovrebbero prendere in considerazione bollettini sulla sicurezza contenenti informazioni importanti relative alle vulnerabilità della sicurezza che potrebbero influire sui sistemi e sui servizi menzionati sopra.
D. SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO	Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?	Il tipo e il volume dei dati personali (scala) possono rendere l'operazione di trattamento dei dati di interesse per gli aggressori (a causa del valore intrinseco di questi dati).
D. SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO	Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?	Le misure di sicurezza specifiche del settore sono solitamente adattate ai bisogni (e ai rischi) del particolare settore. La mancanza di conformità con le migliori pratiche pertinenti potrebbe essere un indicatore di scarsa gestione della sicurezza.

Tabella 3: *domande di valutazione della probabilità*

Seguendo questo approccio, il livello di probabilità di occorrenza della minaccia può essere definito per ciascuna delle aree di valutazione, come segue:

- **Basso**: è improbabile che la minaccia si materializzi.
- **Medio**: c'è una ragionevole possibilità che la minaccia si materializzi.
- **Alto**: la minaccia potrebbe materializzarsi.

Le **tabelle 4 e 5** possono quindi essere utilizzate per documentare la probabilità di occorrenza delle minacce per ciascuna area di valutazione e di conseguenza calcolare il suo valore finale.

AREA DI VALUTAZIONE	PROBABILITA'	
	LIVELLO	PUNTEGGIO
RISORSE DI RETE E TECNICHE	Basso	1
	Medio	2
	Alto	3

PROCESSI / PROCEDURE RELATIVI AL TRATTAMENTO DEI DATI PERSONALI	Basso	1
	Medio	2

AREA DI VALUTAZIONE	PROBABILITA'	
	LIVELLO	PUNTEGGIO
	Alto	3

PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	Basso	1
	Medio	2
	Alto	3

SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO	Basso	1
	Medio	2
	Alto	3

***Tabella 4**: Valutazione della probabilità di occorrenza delle minacce per area*

SOMMA GLOBALE DELLA PROBABILITÀ DI OCCORRENZA DI UNA MINACCIA	LIVELLO DI PROBABILITÀ DELLE MINACCE
4 - 5	Basso
6 - 8	Medio
9 -12	Alto

***Tabella 5**: Valutazione della probabilità di occorrenza di una minaccia*

La probabilità di occorrenza finale della minaccia viene calcolata dopo aver sommato i quattro diversi punteggi ottenuti nella **Tabella 4** e associato il risultato complessivo alle somme globali della **Tabella 5**.

4.2.4 STEP 4: VALUTAZIONE DEL RISCHIO

Dopo aver valutato l'impatto dell'operazione di trattamento dei dati personali e la probabilità di accadimento della minaccia rilavante, la valutazione finale del rischio è possibile (Tabella 6).

		LIVELLO DI IMPATTO		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO**
PROBABILITÀ DI OCCORRENZA DI UNA MINACCIA'	**BASSO**			
	MEDIO			
	ALTO			

Legenda

Rischio basso — Rischio medio — Rischio alto

4.2.5 STEP 5: MISURE DI SICUREZZA

A seguito della valutazione del livello di rischio, l'organizzazione può procedere con la selezione delle misure di sicurezza appropriate per la protezione dei dati personali.

Le **Linee Guida ENISA, nonché il documento Severity Methodology v. 1.0 del 2013,** considerano misure organizzative e tecniche, suddivise in sottocategorie specifiche. In ogni sottocategoria vengono presentate le misure per livello di rischio (basso: verde, medio: giallo, alto: rosso). Al fine di ottenere la scalabilità, si assume che tutte le misure descritte nel livello basso (verde) siano applicabili a tutti i livelli. Allo stesso modo, misure presentate nel livello medio (giallo) sono applicabili anche ad alto livello di rischio. Misure presentate nel livello alto (rosso) non sono applicabili a qualsiasi altro livello di rischio.

4.3 GESTIONE DEL RISCHIO SECONDO LA NORMA UNI/ISO 31000

Sulla base della Norma UNI/ISO 31000, e ai fini della strategia di protezione dei dati personali, viene definita:

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

La gestione del rischio crea e protegge il valore, contribuendo in maniera dimostrabile al raggiungimento degli obiettivi ed al miglioramento della prestazione (per esempio, in termini di salute e sicurezza delle persone, *security*, rispetto dei requisiti cogenti, consenso presso l'opinione pubblica, protezione dell'ambiente, qualità del prodotto gestione dei progetti, efficienza nelle operazioni, *governance* e reputazione). Tale gestione è parte integrante di tutti i processi dell'organizzazione, non essendo un'attività indipendente, separata dalle attività e dai processi principali dell'organizzazione, piuttosto integrando le responsabilità della direzione e i processi dell'organizzazione, inclusi la pianificazione strategica, i processi di gestione dei progetti e del cambiamento.

La gestione del rischio risulta essere parte del processo decisionale e aiuta i responsabili delle decisioni ad effettuare scelte consapevoli, determinare la scala di priorità delle azioni e distinguere tra linee di azione alternative.

La gestione del rischio tratta esplicitamente l'incertezza, tenendo conto esplicitamente dell'incertezza, della natura di tale incertezza e di come può essere affrontata; è sistematica, strutturata e tempestiva contribuendo all'efficienza ed a risultati coerenti, confrontabili ed affidabili sulla base delle migliori informazioni disponibili. Gli elementi in ingresso al processo per gestire il rischio si basano su fonti di informazione quali dati storici, esperienza, informazioni di ritorno dai portatori d'interesse, osservazioni, previsioni e parere di specialisti. Tuttavia, i responsabili delle decisioni dovrebbero informarsi, e tenerne

conto, di qualsiasi limitazione dei dati o del modello utilizzati o delle possibilità di divergenza di opinione tra gli specialisti.

La gestione del rischio è "su misura", in linea con il contesto esterno ed interno e con il profilo di rischio dell'organizzazione, e tiene conto dei fattori umani e culturali, individuando capacità, percezioni e aspettative delle persone esterne ed interne che possono facilitare o impedire il raggiungimento degli obiettivi dell'organizzazione.

La gestione del rischio deve essere trasparente ed inclusiva, coinvolgendo in maniera appropriata e tempestiva i portatori d'interesse (*stakeholders*) e i responsabili delle decisioni, ai vari livelli dell'organizzazione, assicurandone la pertinenza e l'aggiornamento.

La gestione del rischio, infine, deve risultare dinamica e volta al miglioramento continuo dell'organizzazione, rispondendo al cambiamento dovuto ad eventi esterni ed interni, ad un continuo monitoraggio e allo sviluppo di strategie per migliorare la maturità (*maturity*) della gestione del rischio contiguamente agli altri aspetti dell'organizzazione.

La gestione del rischio del trattamento sulla protezione dei dati personali così delineata viene condotta attraverso:

1. l'analisi del rischio, quale fase del processo di gestione, all'interno della quale viene definito il contesto esterno e interno, di natura organizzativa e gestionale;
2. la valutazione del rischio, quale fase del processo di gestione del rischio, all'interno della quale viene identificato, analizzato e ponderato il rischio medesimo.

4.4 VALUTAZIONE DI IMPATTO DEL TRATTAMENTO O DPIA

La valutazione di impatto del trattamento (D.P.I.A., cioè *Data Protection Impact Assessment*) è un onere posto direttamente a carico del titolare del trattamento, col quale si assicura trasparenza e protezione nelle operazioni di trattamento dei dati personali, imponendo al titolare l'onere di una valutazione preventiva delle conseguenze del trattamento dei dati sulle libertà e i diritti degli interessati. Il responsabile del trattamento deve assistere il titolare nella conduzione della DPIA fornendo ogni informazione necessaria.

La valutazione del rischio, da realizzare per ogni singolo trattamento dove la sopracitata analisi avrà evidenziato un livello di rischio alto o comunque laddove sia obbligatorio, ai sensi dell'art. 35 del GDPR, la stessa dovrà portare il titolare a decidere in autonomia se sussistono ancora dei rischi elevati inerenti il trattamento, in assenza dei quali potrà procedere oltre. Se invece riterrà sussistenti detti rischi, dovrà individuare le misure specifiche richieste per attenuare o eliminare il rischio.

Solo nel caso in cui il titolare non dovesse trovare misure idonee a eliminare o ridurre il rischio, occorrerà consultare l'Autorità di controllo. L'Autorità interviene solo *ex post*, sulle valutazioni del titolare, indicando le misure ulteriori eventualmente da implementare, anche con la possibilità di ammonire il titolare o vietare il trattamento.

In ogni caso il titolare dovrà giustificare le sue valutazioni e rendicontarle nel registro dei trattamenti. Il titolare deve consultarsi col DPO (art. 35) quando nominato che ha il compito di fornire, se richiesto, un parere in merito alla valutazione di impatto e sorvegliarne lo svolgimento. Nel caso in cui il titolare non concordi con le indicazioni del DPO dovrà motivare e documentare il suo dissenso.

4.4.1 CASI NEI QUALI LA DPIA È NECESSARIA

L'articolo 35 del regolamento europeo regolamenta la valutazione di impatto, stabilendo la sua necessità quando il trattamento prevede l'uso di nuove tecnologie e / o può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. In particolare, l'articolo 35 GDPR evidenzia la necessità della valutazione di impatto nei seguenti casi:

- il trattamento determina una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici;
- il trattamento riguarda dati sensibili o giudiziari su larga scala;
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Le Autorità di controllo hanno un ruolo importante, in quanto possono stabilire, con un elenco pubblico, quali tipologie di trattamenti richiedono comunque la valutazione di impatto. Allo stesso modo, possono redigere un elenco delle tipologie di trattamenti per i quali la valutazione non è necessaria.

Secondo il **WP248 17 "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" rev. 01 del 4 ottobre 2017**, per meglio determinare la necessità della valutazione di impatto bisogna considerare i seguenti nove criteri:

1) Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (considerando 71 e 91). Esempi di ciò potrebbero includere: un ente finanziario che esamina i suoi clienti rispetto a una banca dati di riferimento in materia di crediti oppure rispetto a una banca dati in materia di lotta contro il riciclaggio e il finanziamento del terrorismo (AML/CTF) oppure contenente informazioni sulle frodi; oppure un'impresa di biotecnologie che offre test genetici direttamente ai consumatori per valutare e prevedere i rischi di malattia o per la salute; oppure un'impresa che crea profili comportamentali o per la commercializzazione basati sull'utilizzo del proprio sito web o sulla navigazione sullo stesso;
2) processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli

interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche" (articolo 35, paragrafo 3, lettera a)). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti delle persone. Il trattamento che non ha effetto o ha soltanto un effetto limitato sulle persone non risponde a questo criterio specifico. Ulteriori spiegazioni in merito a queste nozioni saranno fornite nelle linee guida sulla profilazione che saranno pubblicate prossimamente dal WP29;

3) monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" (articolo 35, paragrafo 3, lettera c))15 . Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);

4) dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10. Un esempio potrebbe essere quello di un ospedale generale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli dei trasgressori. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali documenti personali, messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone;

5) trattamento di dati su larga scala: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala16:
    a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
    b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
    c. la durata, ovvero la persistenza, dell'attività di trattamento;
    d. la portata geografica dell'attività di trattamento;
6) creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato;
7) dati relativi a interessati vulnerabili (considerando 75): il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;
8) uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc. Il regolamento generale sulla protezione dei dati chiarisce (articolo 35, paragrafo 1 e considerando 89 e 91) che l'uso di una nuova tecnologia, definita "in conformità con il grado di conoscenze tecnologiche raggiunto" (considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi. Ad esempio, alcune applicazioni di "Internet delle cose" potrebbero avere un impatto significativo sulla vita quotidiana e sulla vita privata delle persone e, di conseguenza, richiedono la realizzazione di una valutazione d'impatto sulla protezione dei dati;

9) quando il trattamento in sé "*impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto*" (articolo 22 e considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto.

4.4.2 CONTENUTO MINIMO

La valutazione di impatto sulla protezione dei dati deve contenere ai sensi dell'art. 35 § 7 GDPR:

a) Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del Trattamento;
b) Una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) Una valutazione dei rischi per i diritti e le libertà degli interessati di cui al § 1 dell'art. 37;
d) Le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione;

Per come chiarito dal Considerando 84, la D.P.I.A. o Valutazione d'Impatto occorre per "*potenziare il rispetto del […] Regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio*".

4.4.3 RISULTATI DELLA DPIA

Laddove il livello di rischio per i diritti e le libertà degli interessati dovesse risultare significativo, sarà necessario attuare una Consultazione Preventiva del Garante prima di procedere allo specifico trattamento. Se si dimostra, invece, che il rischio è stato efficacemente attenuato delle misure di mitigazione, il processo di valutazione può considerarsi concluso.

4.5 RESPONSABILE PER LA PROTEZIONE DEI DATI (R.P.D. O D.P.O..)

Il Data Protection Officer (DPO), o anche Responsabile per la Protezione dei Dati (RPD), è una figura introdotta dal nuovo Regolamento Europeo 2016/679.

È un consulente esperto, che va ad affiancare il titolare nella gestione delle problematiche del trattamento dei dati personali, in tal modo si garantisce che un soggetto qualificato si occupi in maniera esclusiva della materia della protezione dei dati personali, aggiornandosi sui rischi e le misure di sicurezza, in considerazione della crescente importanza e complessità del settore.

Il ruolo di DPO può essere affidato ad uno dei dipendenti dell'azienda, ma può anche essere esternalizzato a un fornitore di servizi (libero professionista o azienda) tramite apposito contratto, nel qual caso dovrà essere nominato anche responsabile del trattamento. Può essere una persona fisica o un'organizzazione.
Il ruolo del DPO è di tutelare i dati personali, non gli interessi del titolare del trattamento. Deve possedere un'adeguata conoscenza delle normative e delle prassi di gestione dei dati personali, e deve adempiere alle proprie funzioni in piena autonomia ed indipendenza, e in assenza di conflitti di interesse. In tal senso non può ricoprire tale incarico un soggetto che si trovi ai vertici aziendali; quindi, in grado di influenzare le scelte adottate in materia di trattamento dei dati.
Ovviamente, titolare e responsabile devono mettere a disposizione del DPO le risorse umane e finanziarie per poter svolgere il suo compito.

4.5.1 NOMINA E REQUISITI

Il DPO è designato (art. 37) dal Titolare o dal Responsabile del trattamento, in base ad un contratto. La designazione dovrà essere comunicata all'Autorità di controllo nazionale. Tale designazione è obbligatoria solo in tre casi.

a) Per le amministrazioni e gli enti pubblici, autorità pubbliche (eccetto le autorità giudiziarie nell'esercizio delle loro funzioni). Nel regolamento europeo non vi è una definizione di "autorità pubblica, ma il Gruppo Articolo 29 ha raccomandato la nomina del DPO anche per gli organismi privati incaricati dello svolgimento di pubbliche funzioni o che comunque esercitano pubblici poteri (es. forniture elettriche, trasporti pubblici).
b) Se l'attività principale svolta dal titolare o dal responsabile del trattamento consiste nel trattamento di dati che per la loro natura, oggetto o finalità, richiedano il controllo regolare e sistematico degli interessati su larga scala. La nozione di monitoraggio regolare e sistematico include non solo tutti i vari strumenti di tracciatura elettronica e profilazione online, ma anche qualsiasi forma di tracciatura in un ambiente offline.
c) Se l'attività principale consiste nel trattamento su larga scala di dati sensibili, relativi alla salute, alla vita sessuale, genetici, giudiziari e biometrici. Il monitoraggio del comportamento delle persone interessate comprende tutte le forme di monitoraggio e profilazione su Internet, anche ai fini della pubblicità comportamentale.

4.5.2 COMPITI E RESPONSABILITÀ

Il Data Protection Officer ha il compito di informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, sugli obblighi previsti dalle norme in materia e quindi verificarne l'attuazione e l'applicazione. Quindi raccoglie informazioni sui trattamenti svolti, e ne verifica la

conformità alle norme. Se richiesto, potrà fornire pareri ed assistere il titolare in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti.

Inoltre, è il punto di contatto, non solo per il Garante ma anche per gli interessati al trattamento, in merito a qualunque problematica connessa ai loro dati o all'esercizio dei loro diritti. Potrà, infine, consultare il Garante anche di propria iniziativa.

Il DPO non è, però, personalmente responsabile dell'inosservanza degli obblighi in materia di protezione dei dati personali, infatti è compito del titolare (art. 24) mettere in atto le misure tecniche ed organizzative adeguate. Il DPO risponde solo per lo svolgimento dei suoi obblighi di consulenza ed assistenza nei confronti del titolare, che è (eventualmente in solido col responsabile) l'unico soggetto responsabile del rispetto della normativa. Il titolare, quindi, potrà solo avanzare pretese risarcitorie basate sulla responsabilità contrattuale, nei confronti del DPO.

4.5.3 COMUNICAZIONE ALL'AUTORITÀ DI CONTROLLO

In base all'articolo 37, paragrafo 7 del regolamento europeo, il nominativo del DPO eventualmente designato deve essere comunicato all'Autorità di controllo (Garante per la protezione dei dati). Infatti, uno dei compiti principali del DPO è di fare da collegamento con l'Autorità. L'obbligo scatta nel momento in cui si effettua la nomina.

4.6 VIOLAZIONE DEI DATI PERSONALI O *DATA BREACH*

Per violazione dei dati personali (*data breach*) si intende la divulgazione (intenzionale o non), la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati trattati da aziende o pubbliche amministrazioni.

Un "*data breach*", quindi, non è solo un attacco informatico, ma può essere anche un accesso abusivo, un incidente (es. un incendio o una calamità naturale), la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali (furto di un notebook di un dipendente). Il nuovo regolamento europeo prescrive specifici adempimenti nel caso di una violazione di dati personali.

4.5.1 CASI DI NOTIFICA DELLA VIOLAZIONE

La normativa (articolo 33 Regolamento Europeo 2016/679) prevede l'obbligo di comunicare alle autorità di controllo la violazione dei dati, ma solo se il titolare ritiene probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati. Tutti i titolari del trattamento sono soggetti alla norma. La notifica dovrà avvenire entro 72 ore e comunque "*senza ingiustificato ritardo*".

Non è richiesta la comunicazione anche all'interessato nei casi indicati dall'art. 34, cioè quando:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle

destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

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

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

4.5.2 CONTENUTO DELLA NOTIFICA

La notifica deve avere il contenuto previsto dall'art. 33 del Regolamento Europeo 2016/679:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4.5.3 OBBLIGO DI DOCUMENTAZIONE

In ogni caso i titolari dovranno opportunamente documentare le violazioni di dati personali subite, tramite un apposito registro delle violazioni, anche se non comunicate alle autorità di controllo, nonché le conseguenze e i provvedimenti adottati. Il titolare dovrebbe anche documentare nel registro le ragioni delle decisioni assunte, nei casi in cui non ha proceduto alla notifica, ha ritardato la notifica e nei casi in cui non ha comunicato la violazione agli interessati. Tale documentazione dovrà essere fornita al Garante in caso di accertamenti.

Il Registro delle Violazioni, *Data Breach*, è redatto secondo un modello Excel, in cui l'organizzazione dovrà annotare l'accidentale o illecita distruzione, perdita, modifica, accesso, divulgazione non autorizzata, di dati personali. L'organizzazione ne darà tempestiva comunicazione al Garante, qualora vi fosse l'obbligatorietà di notifica.

5. DIRITTI DELL'INTERESSATO

L'interessato (*data subject*) al trattamento è la persona fisica identificata o identificabile, cioè che può essere identificata anche in modo indiretto, facendo riferimento a informazioni o elementi caratteristici, o tramite l'incrocio di più dati personali. Deve essere necessariamente una persona fisica. La normativa attribuisce specifici diritti all'interessato, il quale, per l'esercizio di tali diritti, può rivolgersi direttamente al titolare del trattamento. L'interessato può esercitare i suoi diritti anche in un momento successivo a quello in cui ha prestato il consenso, potendo così revocare un consenso già prestato.

Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibili fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive. Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità.

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

Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. Benché sia il solo titolare a dover dare riscontro in caso di esercizio dei diritti (artt. 15-22), il responsabile è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati (art. 28, paragrafo 3, lettera e).

L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni. Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee.

I diritti esercitabili dall'interessato sono riportati di seguito.

5.1 DIRITTO DI ACCESSO

Il diritto di accesso prevede in ogni caso il diritto di ricevere una copia dei dati personali oggetto di trattamento.

Fra le informazioni che il titolare deve fornire non rientrano le "modalità" del trattamento, mentre occorre indicare il periodo di conservazione previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi.

5.2 DIRITTO ALLA CANCELLAZIONE (OBLIO)

Il cosiddetto diritto "*all'oblio*" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione.
L'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento.

5.3 DIRITTO DI LIMITAZIONE DEL TRATTAMENTO

Il diritto di limitazione (art. 18 del Regolamento) consente all'interessato di ottenere il blocco del trattamento in caso di violazione dei presupposti di liceità (quale alternativa alla cancellazione dei dati stessi), ma anche se l'interessato chiede la rettifica dei dati (in attesa della rettifica) o si oppone al loro trattamento (in attesa della decisione del titolare). Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

5.4 DIRITTO ALLA PORTABILITÀ

Il diritto alla portabilità dei dati è un nuovo diritto previsto dal regolamento europeo. Si applica solo ai trattamenti automatizzati, e sono previste specifiche condizioni per il suo esercizio.
In particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al titolare. Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile, utilizzando anche i formati file più comuni (Excel, di testo, ecc.).

5.5 MODALITÀ DI ESERCIZIO DEI DIRITTI

L'interessato può rivolgersi direttamente al titolare del trattamento per l'esercizio dei suoi diritti (interpello). Anche se è solo il titolare obbligato a dare riscontro, il responsabile del trattamento è tenuto a collaborare col titolare ai fini dell'esercizio dei diritti. In caso di mancata risposta, o di risposta inadeguata, può rivolgersi all'autorità amministrativa (Garante) o giudiziaria per la tutela dei suoi diritti. Il termine per la risposta è di 1 mese per tutti i diritti. Tale termine può essere esteso a 3 mesi in casi di particolare complessità. In questo caso il titolare del trattamento deve comunque avvertire l'interessato

entro il mese. L'esercizio dei diritti è in linea di massima gratuito. Spetta comunque al titolare valutare se la risposta è complessa al punto da dover chiedere un contributo all'interessato, e stabilirne l'ammontare, ma solo se si tratta di richieste manifestamente infondate o eccessive o ripetitive. La risposta si deve fornire di regola in forma scritta, anche attraverso strumenti elettronici. Può essere orale solo se espressamente richiesta in tal senso dall'interessato. La risposta deve essere chiara, coincisa, e facilmente accessibile e comprensibile. Il titolare può chiedere informazioni all'interessato al fine di identificarlo, e l'interessato è obbligato a fornire tali informazioni.

I diritti dell'interessato possono essere esercitati come definito all'interno dell'apposita procedura e relativa modulistica disponibile sul sito web dell'Ente a cui si rimanda.

5.6 TRASFERIMENTO DI DATI ALL'ESTERO

L'intero Capo V (Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali) del regolamento si occupa, della disciplina dei flussi transfrontalieri dei dati personali, e di conseguenza anche dell'utilizzo dei servizi cloud. Tale regolamentazione è lo strumento col quale le leggi dell'Unione europea in materia di protezione dei dati personali interagiscono col resto del mondo.
In caso esistano trattamento con trasferimenti di dati all'estero, questi sono stati mappati, definiti, con indicazione della specifica autorizzazione, nel registro dei trattamenti.

5.7 DIVIETO DI TRASFERIMENTO

Mentre la circolazione dei dati all'intero dello Spazio Economico Europeo (SEE) è libera (art. 12 Convenzione 108), i trasferimenti al di fuori del SEE sono generalmente vietati, a meno che non intervengano specifiche garanzie. L'art. 44 del Regolamento Europeo 2016/679 è chiaro nello stabilire che i trasferimenti di dati personali al di fuori del SEE sono ammessi solo in determinate circostanze. Il regolamento individua due categorie di destinatari in relazione a tale disciplina: gli altri paesi e le organizzazioni internazionali (l'ONU, l'Unesco, e così via).

5.7.1 IPOTESI DI TRASFERIMENTO DATI ALL'ESTERO

In generale il trasferimento di dati personali al di fuori dello Spazio SEE è ammesso se il destinatario garantisce un livello di protezione dei dati adeguato a quello europeo. Il requisito dell'adeguatezza, piuttosto che quello dell'equivalenza, consente l'utilizzo di diverse vie per garantire la protezione dei dati.

1. Decisioni di adeguatezza

Il primo caso nel quale è ammesso il trasferimento di dati all'estero si ha quando il paese terzo garantisce un livello di protezione dei dati adeguato a quello europeo, laddove tale livello di protezione è definito

dalla Commissione europea. Il paese terzo può chiedere alla Commissione di far esaminare la propria legislazione, al fine di ottenere una decisione di adeguatezza (art. 45 Regolamento Europeo 2016/679), o per eventualmente modificare tale legislazione per giungere ad un accordo.

Le decisioni di adeguatezza (elenco delle decisioni di adeguatezza), emanate dalla Commissione europea, sono strumenti vincolanti per i paesi dell'Unione, e in base ad esse è ammesso il trasferimento di dati verso il paese indicato. Le decisioni di adeguatezza possono essere modificate, sospese o revocate, se risulta che il paese terzo non soddisfi più i criteri necessari.

Risultano conformi alle decisioni di adeguatezza i seguenti Paesi: Andorra, Argentina, Australia, PNR, Canada, Faer Oer, Guernsey, Isola di Man, Israele, Jersey, Nuova, Zelanda, Svizzera, Regno Unito e Uruguay.

2. Trasferimento soggetto a garanzie adeguate (clausole standard)

L'art. 46 del Regolamento Europeo 2016/679 prevede un'ulteriore possibilità di trasferimento dei dati personali verso paesi che non garantiscono un adeguato livello di protezione. Il titolare del trattamento di un'azienda basata in Europa, infatti, può stipulare un contratto col titolare dell'azienda che si trova nel paese terzo, le cui clausole sono tali da offrire un livello di protezione adeguato al trattamento dei dati. In particolare, si richiede un soddisfacente livello di sicurezza e la tutela dei diritti degli interessati, con meccanismi di ricorso effettivi.

Non occorre una specifica autorizzazione dell'autorità di controllo nazionale per le seguenti ipotesi:

a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;
b) le norme vincolanti d'impresa in conformità dell'articolo 47;
c) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;
d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;
e) un codice di condotta approvato a norma dell'articolo 40, unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; o
f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.

Occorre, invece, l'autorizzazione dell'autorità di controllo nelle seguenti ipotesi:

a) clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale;

b) disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati.

3. Norme vincolanti di impresa (binding corporate rules)

L'art. 47 prevede uno specifico strumento per il trasferimento di dati personali dal territorio dello Stato tra società facenti parti dello stesso gruppo d'impresa, laddove una di queste sia al di fuori dell'Unione europea. Le **Binding Corporate Rules** (BCR) o norme vincolanti d'impresa (art. 47) si concretizzano in un documento contenente una serie di clausole (*rules*) che fissano i principi vincolanti (*binding*) per tutte le società appartenenti allo stesso gruppo (*corporate*).

Il trasferimento è consentito solo tra aziende che abbiano uno specifico legame societario. Anche in questo caso le clausole devono essere sottoposte alle autorità di controllo, ma è possibile elaborare clausole sulla base di quelle già esistenti e sulle quali già si siano pronunciati i garanti, in modo da avere sufficiente certezza che siano accolte.

5.7.2 DEROGHE ALL'ADEGUATEZZA

Esistono, infine, delle specifiche deroghe alla regola generale dell'adeguatezza, che permettono il trasferimento di dati all'estero (art. 49 Regolamento Europeo 2016/679):

a) l'interessato abbia esplicitamente prestato il proprio consenso al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;
b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;
c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;
d) il trasferimento sia necessario per importanti motivi di interesse pubblico;
e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.

6. AMMINISTRATORE DI SISTEMA

In assenza di definizioni normative e tecniche condivise, l'Amministratore di Sistema viene definito nel **Provvedimento del Garante del 27 novembre 2008 e ss.mm.ii**. come "*una figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise Resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali*".
Deve essere nominato dal Titolare del Trattamento, il quale ha l'obbligo di accertarsi delle capacità tecniche del soggetto cui affida l'incarico e di individuarlo in persona fisica, interna o esterna all'organico dell'Ente, per gli effettivi profili autorizzativi di cui è incaricato.

6.1 COMPITI E FUNZIONI

- È obbligo per il Titolare designare individualmente i singoli amministratori di sistema, a mezzo di un atto che deve elencare analiticamente gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
- I Titolari sono tenuti a riportare in un documento interno (disponibile in caso di accertamenti da parte del Garante) gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad esse attribuite.
- Il Provvedimento richiede che, nel caso in cui i servizi di amministrazione di sistema siano esternalizzati, l'elenco di cui sopra sia conservato, indifferentemente, dal titolare o dal responsabile esterno del trattamento (cioè dall'outsourcer).
- Il Titolare deve adottare idonei sistemi di controllo che consentano la registrazione degli accessi logici da parte degli amministratori ai sistemi di elaborazione e agli archivi elettronici. L'accesso di ciascun amministratore (access log), quindi, deve essere registrato e conservato per almeno 6 mesi, con caratteristiche di completezza, integrità ed inalterabilità e deve comprendere anche i riferimenti temporali, la descrizione dell'evento e del sistema coinvolto.
- Qualora gli amministratori, nell'espletamento delle proprie mansioni, trattino dati personali dei lavoratori, questi ultimi hanno diritto di conoscere l'identità dei predetti. In tal caso, è fatto onere al Titolare di rendere noto ai lavoratori dipendenti detto loro diritto.
- L'operato degli amministratori di sistema deve essere oggetto di verifica, con cadenza almeno annuale, per acclarare che le attività svolte dall'amministratore siano effettivamente conformi alle mansioni attribuite.

6.2 NOMINA DELL'AMMINISTRATORE DI SISTEMA

L'amministratore di sistema è un soggetto interno e/o esterno deputato a:

a) gestire il sistema informatico, nel quale risiedono le banche dati personali, in osservanza al disciplinare tecnico allegato al Codice della privacy e sue successive modifiche ed aggiornamenti, attenendosi anche alle disposizioni del Titolare (e/o del Responsabile, qualora nominato) in tema di sicurezza;

b) monitorare il sistema di sicurezza informatico (idoneo a rispettare le prescrizioni dell'art. 32 del regolamento UE 2016/679 adottato, adeguandolo anche alle eventuali future norme in materia di sicurezza. Più specificatamente, in base al sopra citato vigente disciplinare tecnico, fatte salve le successive integrazioni dello stesso, in qualità di Amministratore di sistema dovrà:

- assegnare e gestire il sistema di autenticazione informatica secondo le modalità indicate nel Disciplinare tecnico e quindi, fra le altre, generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, le parole chiave ed i Codici identificativi personali da assegnare agli incaricati del trattamento dati, svolgendo anche la funzione di custode delle copie delle credenziali;
- procedere, più in particolare, alla disattivazione dei Codici identificativi personali, in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali per oltre 6 (sei) mesi;
- adottare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware, verificandone l'installazione, l'aggiornamento ed il funzionamento degli stessi in conformità allo stesso Disciplinare tecnico;
- adottare tutti i provvedimenti necessari a preservare la riservatezza, l'integrità e la disponibilità dei dati, personali e provvedere al ricovero periodico degli stessi con copie di back-up, vigilando sulle procedure attivate in struttura. L'Amministratore di sistema dovrà anche assicurarsi della qualità delle copie di back-up con attività di *restore* periodici.
- indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego.
- cooperare nella predisposizione del registro dei trattamenti (qualora la Società fosse tenuta alla sua redazione) per la parte concernente il sistema informatico ed il trattamento informatico dei dati;
- vigilare sugli interventi informatici diretti al sistema informatico della Società (se esistente: ...e sull'impianto di videosorveglianza) effettuati da vari operatori esterni. In caso di anomalie sarà sua cura segnalarle direttamente al titolare del trattamento.

- monitorare le misure tecniche ed organizzative di sicurezza per il trattamento informatico dei dati sensibili (se esistenti: e giudiziari) e per la conseguente tutela degli strumenti elettronici;

c) collaborare con il Titolare (e/o con il Responsabile, qualora nominato) per l'attuazione delle prescrizioni impartite dal Garante;

d) comunicare prontamente al Titolare (e/o al Responsabile, qualora nominato) qualsiasi situazione di cui sia venuta a conoscenza che possa compromettere il corretto trattamento informatico dei dati personali;

e) verificare il rispetto delle norme sulla tutela del diritto d'autore sui programmi di elaboratore installati nei pc. presenti nell'unità produttiva, riferendo al Titolare (e/o al Responsabile, qualora nominato).

7. GESTIONE DEL SITO INTERNET

7.1 PRIVACY POLICY

La Privacy Policy è un documento che informa gli utenti dei siti internet circa la gestione e il trattamento dei loro dati personali, sia che si tratti di attività di una vera e propria raccolta dei dati o anche solo del monitoraggio delle visite al sito, mediante strumenti come Google Analytics.

È obbligatoria quando:

- il sito web raccoglie dati personali, come ad esempio nome, cognome, e-mail e il cookie stesso;
- i dati sono raccolti per fini non esclusivamente personali;
- entrano in gioco soggetti terzi, quali ad esempio Facebook e Google.

Deve riportare specifiche informazioni, quali ad esempio:

- la tipologia dei dati raccolti
- il luogo e le finalità del trattamento: è necessario dichiarare gli scopi per cui si raccolgono i dati (per esempio per motivi statistici, di profilazione dell'utente, etc.);
- le modalità di trattamento: il Titolare deve indicare gli strumenti utilizzati per la raccolta dei dati, le modalità di gestione dei dati, le misure preventive e di sicurezza che impediscano ogni tipo di violazione dei dati personali;
- l'identità del Titolare del Trattamento e/o del Responsabile del Trattamento;
- altri soggetti coinvolti (terzi destinatari dei dati);
- i diritti degli interessati (in questo caso, gli utenti): vanno indicate le modalità con le quali l'utente può esercitare i propri diritti;
- la possibilità di produrre il documento anche in lingua inglese, nel caso di utenti stranieri.

L'organizzazione ha applicato e pubblicato la propria privacy policy sul proprio di sito internet.

7.2 COOKIE POLICY

I cookie sono stati introdotti per consentire di memorizzare gli oggetti da acquistare su un dato sito Internet, come gli articoli aggiunti nel carrello della spesa di un negozio online. I cookie, però, possono anche essere utilizzati per ricordare alcune informazioni che l'utente ha precedentemente inserito nei campi di testo di un sito, come ad esempio il nome, l'indirizzo, la password o i numeri delle carte di credito. I cookie sono inoltre usati per memorizzare le ricerche fatte su Internet durante le varie sessioni di navigazione degli utenti. Una legge del 2011 impone a tutti i siti degli stati membri dell'Unione Europea di informare gli utenti che il sito in questione utilizza certe tipologie di cookie.

L'utente verrà informato tramite due livelli di approfondimento: verrà visualizzata una prima informativa breve, a comparsa immediata sulla pagina alla quale l'utente accede, ad esempio tramite banner dinamico, e un'informativa estesa, accessibile tramite un link nell'informativa breve, nonché tramite un link in calce ad ogni pagina del sito aggiornata.

Si precisa inoltre che:

- i siti che non utilizzano cookie non sono soggetti ad alcun obbligo;
- per l'utilizzo di cookie tecnici è richiesta la sola informativa (*ad esempio* nella *privacy policy* del sito) senza banner;
- i cookie analitici sono assimilati a quelli tecnici solo quando realizzati e utilizzati direttamente dal sito prima parte per migliorarne la fruibilità;
- se i cookie analitici sono messi a disposizione da terze parti i Titolari non sono soggetti ad obblighi (notificazione al Garante in primis) qualora:
  - siano adottati strumenti che riducono il potere identificativo dei cookie (*ad esempio* tramite il mascheramento di porzioni significative dell'IP);
  - la terza parte si impegna a non incrociare le informazioni contenute nei cookie con altre di cui già dispone;
  - Ag.I.D. ha raccomandato la piattaforma Web Analytics Italia (WAI), basata sul software open source Matomo, messa a disposizione delle pubbliche amministrazioni per monitorare le statistiche in tempo reale sui visitatori dei propri siti web;
- se sul sito ci sono link a siti terze parti (*es*. banner pubblicitari; collegamenti a social network) che non richiedono l'installazione di cookie di profilazione non c'è bisogno di informativa e consenso;
- nell'informativa estesa il consenso all'uso di cookie di profilazione potrà essere richiesto per categorie (*es*. viaggi, sport);
- è possibile effettuare una sola notificazione per tutti i diversi siti web che vengono gestiti nell'ambito dello stesso dominio;
- gli obblighi si applicano a tutti i siti che installano cookie sui terminali degli utenti, a prescindere dalla presenza di una sede in Italia.

L'organizzazione ha applicato la propria cookie policy sul proprio di sito internet.

7.3 MARKETING E SOFT SPAM

Nel momento in cui il Titolare del Trattamento voglia utilizzare i dati forniti dall'utente per finalità quali l'invio di comunicazioni promozionali relative a servizi forniti dal titolare o addirittura da terzi, nei confronti dei propri clienti. Solo nel caso di cosiddetto "*soft spam*" l'invio è considerato esente da ulteriore consenso, purché sia limitato alle informazioni commerciali relative a servizi analoghi a quelli già eventualmente acquistati dall'interessato.

La normativa pone questa importante eccezione, che però è limitata alle modalità di trasmissione dei messaggi per posta elettronica e non estensibile alle comunicazioni telefoniche, laddove la mail deve essere quella indicata nel contesto della vendita di un prodotto o servizio, e si deve trattare di messaggi inviati a fini di vendita diretta di prodotto e/o servizi forniti dal Titolare (e non da terzi), che devono essere analoghi a quelli già acquistati.

Ulteriore requisito richiesto è che il destinatario non abbia rifiutato all'inizio o nel corso di ulteriori comunicazioni tale invio di comunicazioni promozionali, e che comunque abbia in ogni momento la possibilità di opporsi al trattamento dei dati, gratuitamente e in maniera semplice, e quindi rifiutare l'invio di tali comunicazioni. Nel caso in cui il Titolare voglia utilizzare i dati anche a fini di marketing diretto, deve innanzitutto integrare l'informativa privacy con le informazioni necessarie, e poi richiedere un nuovo e separato consenso. L'Utente, quindi, dovrà poter eventualmente rifiutare il consenso alle comunicazioni commerciali.

8. CLOUD COMPUTING

Sotto il termine "*cloud computing*" si è teso nel corso del tempo a far rientrare qualsiasi servizio o software erogato da sistemi che risiedono fuori dal perimetro aziendale, ma a rigore non tutte andrebbero classificate come servizi cloud. Per loro natura i dati nelle applicazioni cloud sono al di fuori di un controllo diretto. Molto spesso non è possibile garantire che i dati di cui si ha la responsabilità non attraversino effettivamente i confini nazionali o che non siano accessibili da più regioni.

L'impossibilità di garantire sicurezza è dovuta al non conoscere l'esatta localizzazione dei dati e a non sapere chi potrebbe averne accesso. È importante evidenziare che anche se i dati protetti vengono depositati nel cloud si è comunque responsabili della loro protezione.

Se si verifica una violazione dei dati, a prescindere da chi è colpevole, è il Titolare del trattamento che subirà delle sanzioni perché è il soggetto che ha la responsabilità dei dati.

È opportuno che il Gestore del Servizio Cloud garantisca che il trattamento dei dati venga svolto all'interno dell'Unione Europea, aderisca a forme specifiche di garanzie quali Codici di Condotta specifici (ex art. 40 del G.D.P.R., come il **Codice di Condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale**, provv. n. 618 del 17 ottobre 2024 del Garante per la Protezione dei Dati Personali), la quale adesione può essere utilizzata quale criterio di calcolo nelle gare d'appalto, ovvero sia accreditato presso il Catalogo delle Infrastrutture digitali e dei Servizi Cloud dell'Agenzia per la Cybersicurezza Nazionale (A.C.N.), in attuazione del regime ordinario di qualificazione entrato in vigore con il **Regolamento unico per le infrastrutture e i servizi cloud per la PA** (*Decreto Direttoriale n. 21007/24 del 27 giugno 2024*).

8.1 PROCEDURA CAMBIO PASSWORD

Qualora un membro dell'organizzazione debba accedere a reti o programmi che richiedano una sua autenticazione è necessario gestire la consegna della password di accesso e la successiva modifica da parte del lavoratore stesso.

Il titolare del trattamento o l'amministratore di sistema stabilisce un periodo di validità della password di accesso: semestrale in caso di trattamento di dati personali, trimestrale nel caso in cui vengano trattati dati particolari e giudiziari.

Il titolare del trattamento o l'amministratore di sistema assegna al lavoratore una password, che dovrà però essere modificata dallo stesso al primo accesso, mantenendo gli stessi criteri di validità della password (ad esempio nel numero di caratteri o uso di caratteri speciali). In automatico il sistema operativo chiederà all'utente una modifica della chiave di accesso con la periodicità stabilita (3, massimo 6 mesi).

Nel caso in cui il titolare del trattamento o l'amministratore di sistema debbano accedere alla postazione del lavoratore, procederanno alla modifica della password, installandone una provvisoria, che verrà nuovamente modificata dal lavoratore al successivo accesso.

8.2 PROTEZIONE DEI DATI IN FASE DI ARCHIVIAZIONE

Nell'ambito della protezione dei dati personali rileva grande importanza anche la metodologia con cui si procede alla conservazione degli stessi. È necessario prevedere delle misure di sicurezza sia di tipo tecnico che organizzativo, sia a livello fisico/cartaceo, che digitale. Schematizzando si possono elencare:

- misure di tipo organizzativo:

  - politica di sicurezza e procedure di protezione dei dati personali;
  - assegnazione di compiti e responsabilità (nomine);
  - politica di controllo degli accessi;
  - gestione e censimento degli apparati IT;
  - gestione degli incidenti/violazione dei dati personali;
  - obblighi di riservatezza del personale;
  - aumento della sensibilità aziendale nei confronti delle tematiche di tutela dei dati (formazione);
  - conservazione in luoghi diversi dei supporti di backup e archiviazione;

- misure di protezione delle aree e dei locali (criteri di protezione fisica) e rispettive procedure:

  - misure per la protezione dall'accesso intenzionale e non autorizzato ai locali e agli archivi (anti-intrusione);
  - misure per la protezione dei dati da eventi di origine naturale o dolosa (antincendio);
  - misure per la protezione da condizioni ambientali proibitive o da eventuali riduzioni dell'efficienza dei sistemi di supporto (impianti ausiliari);
  - identificazione del personale e dei visitatori;
  - controlli di accesso per zone sicure (registro presenze);
  - misure per la protezione di archivi cartacei (sotto chiave);

- misure di protezione delle architetture di rete, degli applicativi e delle banche dati (criteri di protezione logica dei dati) e relative procedure:

  - misure per la protezione da accessi non autorizzati ad informazioni riservate (User-id, password, screensaver con password);
  - policy specifica per la password (lunghezza, complessità, periodo di validità);
  - misure per la protezione da possibili danneggiamenti alle informazioni (antivirus);
  - sicurezza del server ove risiedono database e applicazioni;
  - sicurezza delle postazioni di lavoro:

- gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza;
- dovrebbe attivarsi il time-out di sessione quando l'utente non è stato attivo per un certo periodo di tempo;
- installazione regolare di aggiornamenti critici rilasciai dallo sviluppatore del sistema operativo;
- sicurezza della rete e delle infrastrutture di comunicazione elettronica (crittografia TLS/ SSL);
- procedure di back-up regolari e monitorate;
- dotazione di livelli di procedure di controllo degli accessi per i dispositivi mobili e portatili;
- sicurezza del ciclo di vita delle applicazioni;
- smaltimento o riutilizzo sicuro di supporti informatici;
- crittografia dei sistemi wireless;
- monitoraggio dell'accesso da remoto da parte di un amministratore IT;
- periodici test di penetrazione, per verifica vulnerabilità tecnica;

8.3 CANCELLAZIONE SICURA DELLE INFORMAZIONI

Il problema dell'*e-waste* riguarda chiunque mantenga memorizzati su dispositivi elettronici dati relativi a sé o a terzi: è infatti compito del loro possessore dati assicurare che questi non possano andare dispersi e acquisiti anche in modo incontrollato da estranei.

La semplice cancellazione dei file o la formattazione dell'hard-disk, infatti, non sempre realizzano una vera cancellazione delle informazioni registrate, che rimangono spesso fisicamente presenti e tecnicamente recuperabili.

Per prevenire l'acquisizione indebita di dati è necessario operare in diversi modi e tempi a seconda delle circostanze:

- immediatamente prima della cessione o dismissione dell'apparato elettronico, con strumenti software di cancellazione sicura (a condizione che l'apparato sia funzionante);
- al momento della cessione o dismissione, con la demagnetizzazione (degaussing), che azzera tutte le aree di memoria elettronica e rende l'apparato inutilizzabile, o con la distruzione fisica del dispositivo di memorizzazione.

Per ciascuna delle opzioni citate si forniscono qui di seguito delle informazioni per la messa in pratica o per il reperimento di informazioni più dettagliate.

8.3.1 DEMAGNETIZZAZIONE E DISTRUZIONE

Nel caso in cui il dispositivo elettronico da sottoporre a smaltimento non sia più funzionante, e non siano pertanto applicabili le misure software, allo scopo di garantire l'impossibilità di recupero dei dati da parte di terzi estranei occorre procedere con modalità hardware, basate sull'uso di dispositivi di demagnetizzazione (*degausser*), o con la distruzione fisica.

I *degausser* permettono l'"azzeramento" delle aree magnetiche delle superfici dei dischi o di altre memorie a stato solido, agendo anche sui circuiti elettronici che fanno parte del dispositivo e causandone l'inutilizzabilità successiva.

In determinati casi è necessario ricorrere alla distruzione fisica dei dispositivi di memoria. Tale procedura è l'unica praticabile con i supporti ottici a sola lettura (CD-ROM, DVD-R), che possono essere distrutti o polverizzati con apposite macchine analoghe ai "*trita-carta*" in uso negli uffici. Gli hard-disk possono essere resi inutilizzabili aprendone l'involucro protettivo e danneggiando meccanicamente le superfici magnetiche (*piatti*) con l'azione deformante di uno strumento o con appositi punzonatori.

8.3.2 DISTRUZIONE DI DOCUMENTI CARTACEI

La distruzione di documenti cartacei può essere effettuata a mezzo di sistemi "trita-carta". I più sicuri sono quelli che riducono la carta in coriandoli e che non consentono, quindi, di ricostruire il documento.

Se le quantità di carta da distruggere sono significative può essere necessario rivolgersi a soggetti che svolgono professionalmente tale attività acquisendo il relativo certificato di avvenuta distruzione, con il relativo Accordo di nomina a Responsabile Esterno del Trattamento ai sensi dell'art. 28 del G.D.P.R. con apposite istruzioni di riservatezza.

9. VIDEOSORVEGLIANZA

Il Provvedimento generale dell'8 aprile 2010 e le Linee Guida Europee 3/2019 sul trattamento dei dati personali attraverso dispositivi video, fissano i requisiti per evitare che l'attività di videosorveglianza possa diventare una minaccia per i diritti degli interessati.
Quindi, il Garante ha stabilito che l'attività di videosorveglianza è consentita se sono rispettati i seguenti principi:

- liceità;
- necessità;
- proporzionalità;
- finalità.

La videosorveglianza è lecita se è funzionale allo svolgimento delle funzioni istituzionali, quando si tratta di enti pubblici, oppure, nel caso di privati o enti pubblici economici, se sono rispettati gli obblighi di legge (in particolare le norme del codice penale che vietano le intercettazioni di comunicazioni e conversazioni: art. 615 bis C.P.) e il provvedimento del Garante in materia di bilanciamento degli interessi, oppure se vi è un consenso libero ed espresso da parte delle persone riprese dalle telecamere.
Il Titolare del Trattamento ha approvato con Delibera di Consiglio Comunale n. 18 del 31.03.2022 il "Regolamento di Videosorveglianza" stabilendo la garanzia "*che il trattamento dei dati personali, effettuato mediante l'attivazione dell'impianto di videosorveglianza nel territorio urbano ed extraurbano di Comune di Fiano Romano (RM)"* sia "*gestito in piena autonomia e nel rispetto delle norme vigenti dal personale (Ufficiali/Agenti) del Comando di Polizia Locale*" per le finalità stabilite dall'art. 3.

Installazione degli impianti

Per installare un impianto di videosorveglianza non è necessario ottenere il consenso preventivo dei soggetti ripresi, purché siano rigorosamente rispettate le modalità indicate dal Garante e servano a tutelare beni e persone da aggressioni o a prevenire incendi o a garantire la sicurezza del lavoro. Occorre, quindi, apporre preventivamente un cartello (informativa), sul modello indicato dal Garante, che avverte i cittadini quando entrano in una zona controllata da telecamere. Il cartello deve essere apposto prima dell'inizio dell'area delle riprese, deve essere chiaramente visibile anche di notte, e indicare la finalità delle registrazioni (il cartello deve essere correttamente compilato). Se le immagini sono inviate alle autorità di polizia, tale circostanza deve essere indicata nel cartello-informativa.

MODELLO SEMPLIFICATO CARTELLO VIDEOSORVEGLIANZA

(EDPB - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - adottate il 29 gennaio 2020)

Le telecamere istallate a fini di tutela dell'ordine e della sicurezza pubblica non devono essere segnalate, ma il Garante auspica comunque l'utilizzo di cartelli che informino i cittadini.

L'installazione di impianti di videosorveglianza deve essere realizzata in modo da evitare trattamenti di dati non necessari. Alcuni impianti necessitano di una verifica preliminare da parte del Garante, come quelli che incrociano le immagini con altri dati, tipo i dati biometrici oppure i codici identificativi delle carte elettroniche, o le rilevazioni della voce. Se l'impianto rileva dati sensibili o giudiziari, come accade per le persone malate o i detenuti, è necessaria l'autorizzazione del Garante, come anche nel caso di sistemi che interpretano le azioni dei cittadini, i gesti, e segnalano eventi o comportamenti anomali.

Il titolare del trattamento deve nominare per iscritto le persone fisiche incaricate del trattamento che possono accedere ai dati trattati, laddove il numero di tali soggetti deve essere limitato e la visione delle immagini deve essere consentita solo se è indispensabile per gli scopi perseguiti. Quindi l'accesso al monitor dove sono visibili le immagini deve essere esclusivamente limitato alle persone designate. L'ideale è che i monitor siano installati in locale separato e chiuso. Deve ritenersi non conforme alle norme la prassi di rivolgere le telecamere al pubblico.

Le immagini registrate non possono essere conservate più a lungo di quanto necessario per le finalità per le quali sono acquisite (art. 5, paragrafo 1, lett. c) ed e), del Regolamento). In base al principio di responsabilizzazione (art. 5, paragrafo 2, del Regolamento), spetta al titolare del trattamento individuare i tempi di conservazione delle immagini, tenuto conto del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. Ciò salvo che specifiche norme di legge non prevedano espressamente determinati tempi di conservazione dei dati (si veda, ad esempio, l'art. 6, co. 8, del D.L. 23/02/2009, n. 11, ai sensi del quale, nell'ambito dell'utilizzo da parte dei Comuni di sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana, "la conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione").

Tenendo conto dei principi di minimizzazione dei dati e limitazione della conservazione, i dati personali dovrebbero essere – nella maggior parte dei casi (ad esempio se la videosorveglianza serve a rilevare atti vandalici) – cancellati dopo pochi giorni, preferibilmente tramite meccanismi automatici. Quanto più prolungato è il periodo di conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l'analisi riferita alla legittimità dello scopo e alla necessità della conservazione.

Un periodo di conservazione di 24 ore è quindi sufficiente. La chiusura nei fine settimana o in periodi festivi più lunghi potrebbe tuttavia giustificare un periodo di conservazione più prolungato.

Gli interessati, cioè i soggetti ripresi, devono poter accedere alle riprese che li riguardano e verificare le modalità di utilizzo dei dati raccolti. L'illiceità delle riprese comporta non solo l'inutilizzabilità delle registrazioni, ma anche il provvedimento di blocco e divieto di trattamento dei dati, da parte del Garante. In casi estremi si possono configurare anche reati penali.

9.1 VIDEOSORVEGLIANZA ALL'INTERNO DEI LUOGHI DI LAVORO

L'art. 4 dello Statuto dei Lavoratori Legge n. 300/70 vieta l'utilizzo di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. Impianti e apparecchiature di controllo possono essere installati solo per motivi di sicurezza dell'attività economica, intesa sia come integrità dell'azienda nel suo complesso, sia come integrità delle persone che vi operano, titolari o dipendenti, o dei cittadini che si trovino ad accedere ai locali dell'impresa.

Qualora l'installazione di impianti di controllo per motivi di sicurezza comporti la possibilità di controllo a distanza dell'attività dei lavoratori, è necessario che Prima di procedere all'installazione dell'impianto l'azienda stipuli apposito Accordo con le rappresentanze sindacali aziendali (o in mancanza con la commissione interna) o, in mancanza, inoltri alla Direzione Provinciale del Lavoro competente per territorio apposita istanza per il rilascio dell'autorizzazione.

Nell'istanza di rilascio autorizzazione devono essere specificate le motivazioni dell'installazione ed indicate le caratteristiche tecniche dell'impianto audiovisivo.

L'istanza deve essere presentata in bollo, unitamente a:

- copia dell'informativa consegnata ai dipendenti e da loro sottoscritta;
- documentazione tecnica dell'impianto;
- n. 1 marca da bollo per il provvedimento autorizzatorio;
- non possono essere autorizzati gli impianti in cui il cono di azione delle telecamere comprenda:
    - luoghi riservati esclusivamente ai lavoratori (es. postazioni di lavoro fisse) o non destinati all'attività lavorativa (es. luoghi per la fruizione della pausa, bagni, spogliatoi, ecc.);
    - locali in cui sia posizionato il sistema di rilevazione delle presenze (marcatempo).

Gli adempimenti da assolvere sono:

- preventivo accordo con le rappresentanze sindacali aziendali o preventiva istanza di autorizzazione alla Dpl;
- informativa ai dipendenti circa l'installazione dell'impianto;
- obbligo di informare dipendenti e clienti con appositi cartelli da appendere dentro e fuori i locali dell'azienda;
- obbligo di nomina dell'incaricato alla videosorveglianza;
- installazione di videocamere il cui angolo di ripresa inquadri solo le parti a rischio di rapina o di altri comportamenti criminosi e comunque nel rispetto della normativa sulla privacy;
- la ripresa dei dipendenti deve essere occasionale e finalizzata esclusivamente alla sicurezza aziendale;
- le telecamere dovranno essere dotate possibilmente di spia luminosa che individui quando le stesse sono in funzione;
- l'apparecchiatura di registrazione deve essere opportunamente custodita ed accessibile solo da parte dell'incaricato alla videosorveglianza;
- le registrazioni possono essere visionate solo in caso di presunti fatti delittuosi (presunte violazioni per furti, danneggiamenti ed atti di vandalismo) in presenza, oltre che dell'incaricato alla videosorveglianza, dell'autorità giudiziaria intervenuta sul luogo a seguito di denuncia.

Ricevuta l'istanza, la procedura di rilascio dell'autorizzazione da parte della Direzione Prov.le del Lavoro si articola nel seguente modo:

- un ispettore effettua un sopralluogo in azienda;
- visiona la planimetria ed i luoghi di installazione delle telecamere;
- interroga il titolare ed il personale presente;
- effettua una relazione al proprio Dirigente, propedeutica al provvedimento autorizzativo.

Se all'atto dell'accesso ispettivo, l'ispettore riscontra che l'azienda ha installato e messo in uso un impianto audiovisivo che consente il controllo a distanza dei lavoratori senza la preventiva autorizzazione della D.p.l., rileva una violazione.

In ultima istanza, in tema di sorveglianza datoriale, è da considerare il **provv. n. 364 del 6 giugno 2024 emanato dal Garante per la Protezione dei Dati Personali** "**Documento di indirizzo, Programmi e servizi informatici di gestione della posta elettronica del contesto lavorativo e trattamento dei metadati**" che fa riferimento ai "*metadati*", definiti come "*informazioni registrate nei log generati dai sistemi server di gestione e smistamento della posta elettronica (MTA = Mail Transport Agent) e dalle postazioni nell'interazione che avviene tra i diversi server interagenti e, se del caso, tra questi e i client (le postazioni terminali che effettuano l'invio dei messaggi e che consentono la consultazione della corrispondenza in entrata accedendo ai mailbox elettroniche, definite negli standard tecnici quali MUA – Mail User Agent)*". Il Garante ha sottolineato la necessità, non prescrittiva, da parte dei Titolari del Trattamento di limitare la conservazione dei metadati, riferiti *all'envelope* delle comunicazioni elettroniche dei dipendenti, ad un massimo di giorni 21. "*Nell'ambito della […] finalità (assicurare il funzionamento delle infrastrutture del sistema della posta elettronica), a cui risulta applicabile il comma 2 dell'art. 4 della L. n. 300/1970, l'eventuale conservazione per un termine ancora più ampio potrà essere effettuata, solo in presenza di particolari condizioni che ne rendano necessaria l'estensione, comprovando adeguatamente, in applicazione del principio di accountability previsto dall'art. 5, par. 2, del Regolamento, le specificità della realtà tecnica e organizzativa del Titolare*". Diversamente, la raccolta generalizzata e la conservazione indefinita dei log di posta elettronica potrebbe comportare un controllo a distanza indiretto dell'attività dei lavoratori.

10. DOCUMENTAZIONE DEL SISTEMA DI PROTEZIONE – ALLEGATI

Le diverse componenti del sistema di protezione sono documentate almeno da:

1. Modello di Organizzazione per la Protezione dei Dati Personali e Gestione del Rischio di Violazione – brevemente denominato "*Modello Organizzativo Privacy*" rappresentato dal presente documento;
   - 1.1. Registro delle attività di trattamento dei dati, art. 30 del G.D.P.R. contenente relativo esito dell'analisi del rischio e relativi trattamenti a rischio alto;
   - 1.2. Format per Nomine dei Soggetti Designati, art. 29 del G.D.P.R. e art. 2-quaterdecies D.Lgs. n. 196/2003;
   - 1.3. Format per Nomine dei Soggetti Autorizzati, art. 2-quaterdecies D.Lgs. n. 196/2003;
   - 1.4. Format per Accordo di Responsabilità Esterna del Trattamento ex art. 28 G.D.P.R. ;
   - 1.5. Format per Accordo di Responsabilità Esterna del Trattamento per Professionisti ex art. 28 G.D.P.R;

1.6. Informativa Estesa per l'Accesso agli Atti ex L. 241/1990;
1.7. Modulo di Esercizio dei Diritti dell'Interessato del Trattamento per i diritti di cui al Capo III del G.D.P.R.
1.8. Misure minime di sicurezza ICT per le Pubbliche Amministrazioni, Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015, Ag.I.D. ;

Sono ulteriormente ricomprese all'interno del sistema di protezione dei dati personali del Titolare del Trattamento, gli ulteriori documenti che si elencano e seguiranno:

- (A) Template Nomina ad Amministratore di Sistema
- (B) Template Accordo di Riservatezza
- (C) Template Informativa Servizi
- (D) Informativa al Dipendente
- (E) Informativa al Fornitore
- (F) Informativa al Professionista
- (G) Procedura per l'Esercizio dei Diritti dell'Interessato
- (G1) Modello per l'Esercizio dei Diritti dell'Interessato
- (H) Misure di Sicurezza e Organizzative del Titolare del Trattamento
- (I) Template di Accordo Sindacale
- (L) Policy per la Distruzione e/o Reimpiego delle Apparecchiature Elettroniche
- (M) Dicitura (Informativa) Breve per modulistica
- (N) Template Nomina per Responsabile Esterno Professionista
- (O) Clausola Contrattuale Trattamento dei Dati Personali