**ALLEGATO 1**

UNIONCAMERE

# SGDP - SISTEMA DI GESTIONE DEI DATI PERSONALI
# Modello organizzativo, ruoli e sistema di responsabilità

ai sensi del Regolamento UE 679/2016

## SOMMARIO

# PREMESSA

## SCOPO E CAMPO DI APPLICAZIONE

Scopo del presente documento è definire il modello organizzativo per la gestione degli adempimenti "sistemici" in materia di protezione dei dati e degli interessati, avendo come riferimento il Regolamento UE 2016/679 sulla protezione dei dati personali, (di seguito Regolamento UE o GDPR) ed i provvedimenti emanati nel tempo dal Garante per la protezione dei dati personali (di seguito anche "Garante Privacy" o "Garante").
In particolare, il documento regolamenta:

a) i **ruoli e le responsabilità** assegnate ai vari livelli gestionali, di controllo ed operativi, al fine di garantire la corretta tenuta del predetto modello e, di conseguenza, la compliance alla normativa di riferimento;
b) le modalità per il rilascio delle necessarie **istruzioni** ai soggetti autorizzati, ai vari livelli, al trattamento dei dati personali;
c) gli strumenti per il **monitoraggio e controllo** del sistema, al fine di garantire il miglioramento continuo dello stesso ed il mantenimento della compliance;
d) l'iter per il riesame e la verifica di adeguatezza periodica del SGDP e le regole generali per l'**aggiornamento** dello stesso.

Il presente documento è portato a conoscenza, anche attraverso attività di sensibilizzazione o formazione, a tutti i Dirigenti, Quadri, funzionari o, comunque, referenti delle Aree/Servizi/Uffici di Unioncamere potenzialmente coinvolti nella stessa.

## RIFERIMENTI NORMATIVI

Il presente documento risponde ai seguenti requisiti normativi:

1. Titolare del trattamento (art. 4, n. 7 e 24 del GDPR);
2. Responsabile della Protezione dei Dati (art. 37 e ss. del GDPR);
3. Soggetti che trattano dati "per conto" e sotto l'autorità del Titolare del trattamento (art. 29 del GDPR);
4. Attribuzione di funzioni e compiti a soggetti designati (art. 2-quaterdecies del D.Lgs. 196/2003 e s.m.i.)
5. Garante per la protezione dei dati personali, Comunicato 11 dicembre 1997 "Privacy: chi sono i titolari e i responsabili del trattamento dei dati nelle imprese e nelle amministrazioni pubbliche";
6. WP29, Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento";
7. Garante per la protezione dei dati personali, Provvedimento del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e s.m.i.

## ACRONIMI E DEFINIZIONI UTILIZZATE

| | |
|---|---|
| GDPR | Regolamento UE 2016/679 (General Data Protection Regulation) |
| Codice | D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. 101/2018 |
| Garante | Garante per la protezione dei dati personali |
| WP29 | Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo della protezione dei dati) |
| RPD/DPO | Responsabile della Protezione dei Dati |
| Delegato del Titolare | Soggetto che, secondo le deleghe/procure formalizzate ed il sistema di gestione della privacy, garantisce specifiche funzioni ai fini della *compliance* al GDPR |
| SG | Segretario Generale di Unioncamere |
| RSGQ | Responsabile del Sistema di Gestione della Qualità di Unioncamere |
| | |

## MATRICE DELLA REDAZIONE E DELLE REVISIONI

| Data | Stato | Descrizione | Approvazione |
|---|---|---|---|
| 13/12/2018 | Approvato | Rev 0 – I$^{a}$ emissione | Delibera del Comitato esecutivo del 13/12/2018 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## CONTESTO ORGANIZZATIVO DI RIFERIMENTO

Unioncamere - Unione italiana delle Camere di commercio, industria, artigianato e agricoltura - è l'ente pubblico che unisce e rappresenta istituzionalmente il sistema camerale italiano.

La mission di Unioncamere è definita direttamente dall'art. 7 della Legge n. 580/1993 e s.m.i.

La Struttura organizzativa è definita dallo Statuto e dal Regolamento di Organizzazione (in quanto ad articolazione delle funzioni e responsabilità ai vari livelli), da appositi Ordini di servizio in quanto alla strutturazione della stessa in Aree, Servizi ed Uffici (centri di responsabilità primari e secondari). Per l'identificazione della Struttura vigente nel tempo, si rinvia alla specifica sezione del sito istituzionale "Amministrazione trasparente"[1].

Unioncamere ha strutturato da tempo l'articolazione delle responsabilità interne in materia di protezione dei dati, originariamente nell'ambito del proprio Documento Programmatico sulla Sicurezza approvato periodicamente dagli Organi, successivamente con specifica delibera del Comitato esecutivo n. 153 del 27/11/2013.

La ridefinizione dell'assetto delle responsabilità in materia di gestione dei dati personali si rende ora necessario:

a) per effetto delle modifiche apportate al sistema gestionale interno che, ai sensi del D.Lgs. 196/2003 prevedeva due figure: una opzionale, il responsabile del trattamento (art. 29), finora coincidente con i Dirigenti di ciascuna Area organizzativa e, per le funzioni di staff, con il Segretario Generale; una obbligatoria, l'incaricato del trattamento (art. 30); in tal senso, il Regolamento UE esemplifica il quadro di riferimento, in quanto:
   - con il termine "responsabile del trattamento", l'art. 28 del GDPR, si riferisce esclusivamente a soggetti esterni all'organizzazione del Titolare, che operano sulla base di un contratto o atto giuridico analogo;
   - tutti gli ulteriori soggetti che abbiano accesso a dati personali, non possono trattarli se non previo rilascio di adeguate istruzioni (art. 30 del GDPR);

   Sul punto, il D.Lgs. 101/2018 di armonizzazione del quadro normativo interno al GDPR ha parzialmente abrogato e modificato il D.Lgs. 196/2003 prevedendo (art. 2-quaterdecies) la possibilità che
   - specifici compiti e funzioni connessi al trattamento di dati personali possano essere attribuiti, nell'ambito dell'assetto organizzativo vigente, a persone fisiche, espressamente designate, che operano sotto l'autorità e responsabilità del Titolare del trattamento
   - le persone che operano sotto l'autorità diretta del Titolare possano essere autorizzate al trattamento con le modalità ritenute più opportune dal Titolare stesso;
b) previsione di una nuova funzione, il Data Protection Officer (o Responsabile della Protezione dei Dati – RPD/DPO) che assomma le funzioni di cui all'art. 39 del GDPR (sostanzialmente, supporto al titolare del trattamento e verifica/controllo delle politiche implementate);
c) in ragione della complessità delle funzioni svolte e delle relazioni istituzionali con altri Organismi pubblici e Organizzazioni private, che comporta la revisione (anche in funzione dell'autonomia gestionale propria delle figure apicali ai vari livelli) e riallocazione delle responsabilità ai fini della più complessiva compliance al GDPR.

Per queste motivazioni, **per effetto dell'approvazione del presente modello organizzativo**, nell'ambito della più generale governance di Unioncamere, è promossa un'articolazione **"a rete"** delle funzioni e competenze di gestione e controllo in materia di privacy compliance. In tale contesto, i processi coordinati a livello centrale dal Titolare del trattamento coadiuvato dal Data Protection Officer, trovano attuazione all'interno della Struttura organizzativa attraverso:

a) un livello dirigenziale, a cominciare dal Segretario generale, con autonomia gestionale ed organizzativa, nell'ambito delle politiche generali definite dal Comitato esecutivo, che riferiscono direttamente al Titolare ("**Delegati del Titolare**"); a tali soggetti, da considerarsi designati ai sensi dell'art. 2-quaterdecies, co. 1 del D.Lgs. 196/2003 per effetto della documentata preposizione alla direzione di una Area organizzativa dirigenziale, sono affidati specifici compiti e funzioni connessi al trattamento dei dati personali di competenza successivamente delineati;
b) la nomina del **Responsabile della protezione dei dati**, con funzioni di supporto al Titolare del trattamento e di monitoraggio e controllo del sistema implementato;
c) i meccanismi e modalità per **l'identificazione ed autorizzazione degli ulteriori soggetti** che, sotto la diretta autorità del Titolare e dei Delegati di cui alla precedente lett. a), effettuano i trattamenti di dati personali.

[1] http://www.unioncamere.gov.it/P42A1943C1921S1919/articolazione-degli-uffici.htm

## RUOLI E RESPONSABILITÀ

### TITOLARE DEL TRATTAMENTO

L'interpretazione da sempre avallata dal Garante per la protezione dei dati personali prevede che il meccanismo di imputazione delle responsabilità in materia di privacy sia mutuato dallo schema organizzativo in concreto adottato dall'ente con riguardo alle potestà decisionali.

In linea con tale interpretazione e sulla base della lettura delle competenze istituzionali degli organi di vertice di Unioncamere e ferma restando la qualifica di *Titolare del trattamento* da **identificarsi nella struttura nel suo complesso e, quindi, in capo a Unioncamere**, le funzioni di natura gestionale che la legge attribuisce al *Titolare*, non possono che essere originariamente individuate in capo al **Comitato esecutivo** che, a mente dell'art. 6 dello Statuto è organo amministrativo e di indirizzo politico.

In tal senso, si ritiene che il Comitato esecutivo, in materia debba determinare - considerando la natura, l'ambito di applicazione, il contesto, i rischi per i diritti e le libertà degli interessati - le finalità e le modalità del trattamento, assicurando che venga adottato un sistema di gestione degli adempimenti privacy ed adeguate misure (tecniche ed organizzative) di sicurezza, in conformità ai requisiti del Regolamento ed ai principi di accountability e di privacy by design & by default. In considerazione di tali funzioni, il Comitato Esecutivo provvede:

a) a nominare il **Responsabile della Protezione dei Dati (RPD/DPO);**
b) ad approvare i **principali documenti gestionali** per il regolare ed efficiente funzionamento del sistema privacy di Unioncamere ovvero:
   - ✓ il presente modello organizzativo;
   - ✓ il registro dei trattamenti;
   - ✓ la procedura di gestione dei data breach;
   - ✓ gli altri documenti a carattere generale.
c) a conferire **espressa delega** ai dirigenti dell'ente per la gestione dei vari adempimenti rilevanti, anche per rinvio alle funzioni previste dal presente modello;
d) ad adottare tutte le **decisioni** che eventualmente non rientrino nelle competenze ordinarie e nei limiti di spesa del segretario generale, ovvero conferite ai "delegati";
e) **a riesaminare ed aggiornare** periodicamente, avvalendosi del Responsabile della Protezione che riferisce direttamente al citato organismo, le misure a tutela degli interessati ai fini della compliance generale dell'Ente al GDPR.

### RESPONSABILE DELLA PROTEZIONE DEI DATI

Con delibera n. 12 del 14 febbraio 2018, il Comitato Esecutivo ha proceduto alla nomina del Responsabile della Protezione dei Dati di Unioncamere, nella persona del vice segretario generale, Responsabile dell'Area legale dell'Ente, in possesso quindi sia di specifiche qualità professionali, nonché di caratteristiche di indipendenza, autorevolezza e competenze manageriali.
All'RPD di Unioncamere è stato affidato il compito:

a) di assistere il Titolare durante tutto l'iter di analisi e valutazioni preventive per l'adozione del nuovo modello organizzativo, nonché di esercitare le funzioni di cui agli artt. 37 e ss. del GDPR nei confronti della stessa Unioncamere;
b) di agire quale facilitatore nell'ambito dei programmi di adeguamento, da parte delle Camere di commercio, e degli altri organismi del sistema camerale, dei propri modelli organizzativi alle prescrizioni normative del nuovo Regolamento UE 2016/679 coordinando, ove necessario, le altre strutture del sistema camerale che assistono e supportano le Camere di commercio in tali attività;
c) di coordinare l'Unità di progetto "DPO camerali", cui afferiscono alcuni dipendenti di Unioncamere che, adeguatamente formati, svolgono il ruolo di RPD/DPO presso le Camere di Commercio che abbiano richiesto tale servizio.

Per quanto attiene ai compiti sub a), oggetto di disciplina nell'ambito del presente modello, i compiti di cui all'art. 39 del GDPR si traducono operativamente nell'esercizio delle seguenti funzioni:

- supportare il Titolare del trattamento nel percorso di implementazione del GDPR a livello organizzativo-gestionale e tecnico-informatico, sia in fase di avvio (provvedendo a valutare la "consistenza" del registro dei trattamenti e dell'assessment formalizzato anche al fine di supportare la definizione di eventuali misure idonee di cui sia indispensabile programmare l'implementazione), che per tutta la durata dell'incarico (esprimere formale parere sui documenti di carattere gestionale e sulle soluzioni tecnico-informatiche che verranno progettate per la compliance generale di Unioncamere);
- informare e consigliare il Titolare del trattamento, i dirigenti ed i dipendenti sugli obblighi derivanti dal GDPR e

dalla normativa nazionale; in questo ambito, all'RPD potrà essere richiesto di partecipare ad incontri operativi ai vari livelli in cui vengano assunte decisioni relative al trattamento dei dati personali;

- sorvegliare l'osservanza del GDPR e delle politiche interne in materia di protezione dei dati, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale, anche attraverso la conduzione di audit e visite ispettive programmate e/o a sorpresa;
- fornire se richiesto un parere sulla valutazione d'impatto del trattamento sulla protezione dei dati di cui agli artt. 35 e ss. del Regolamento, in particolare: sorvegliandone lo svolgimento, provvedendo ad esaminarne gli esiti finali e supportando le decisioni connesse agli obblighi di consultazione preventiva del Garante;
- partecipare alle istruttorie e valutazioni circa eventuali violazioni di dati personali occorsi presso Unioncamere, supportando il Titolare nelle decisioni circa la gestione delle notificazioni dei data breach di cui agli artt. 33 e 34 del GDPR secondo quanto previsto nell'apposita procedura gestionale;
- con riferimento al punto precedente, anche avvalendosi della propria struttura di supporto, provvedere alla istituzione, alimentazione ed aggiornamento del "Registro dei data breach" come previsto da apposita procedura gestionale (in allegato 1 al presente documento);
- cooperare con il Garante italiano e con quello di eventuali paesi esteri con cui l'Unioncamere dovesse entrare in contatto, e fungere da punto di riferimento per facilitare l'accesso, da parte di questa, ai documenti ed alle informazioni necessarie ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi alla stessa attribuite dal GDPR;
- fungere da punto di contatto e curare i rapporti con gli interessati, coinvolgendo i dirigenti competenti *ratione materiae* nell'analisi ed evasione di ogni questione[2] che venga sottoposta direttamente alla propria attenzione ovvero all'attenzione del Titolare del trattamento; in proposito si specifica che, pur nel caso in cui la richiesta di esercizio dei diritti sia sottoposta al RPD, la decisione sul riconoscimento o meno del diritto – e la relativa comunicazione all'interessato – spetta esclusivamente al Titolare
- con riferimento al punto precedente, anche avvalendosi della propria struttura di supporto, provvedere alla istituzione, alimentazione ed aggiornamento del "Registro delle richieste di esercizio dei diritti degli interessati" (in allegato 2 al presente documento);
- formalizzare periodiche relazioni al Titolare del trattamento (Comitato Esecutivo) contenenti la descrizione delle attività di supporto interno e di controllo effettuate, il resoconto relativo all'implementazione delle misure suggerite, nonché una valutazione generale e specifica sulla compliance di Unioncamere al GDPR.

Il perimetro d'intervento del RPD comprende tutti i trattamenti di dati personali posti in essere da Unioncamere, compresa l'attività eventualmente delegata a soggetti (persone fisiche e giuridiche).

L'RPD riferirà direttamente alla governance del Titolare del trattamento (Comitato Esecutivo, Presidente Unioncamere e Segretario generale) a seconda delle circostanze e delle prerogative specifiche degli Organi (ad es., decisioni strategiche/operative ovvero caratterizzate da urgenza) anche sulla base della ripartizione dei compiti e delle responsabilità interne ad Unioncamere specificamente definite nel prosieguo del presente documento.

Al fine di garantire i necessari requisiti di autonomia ed indipendenza nell'esecuzione dell'incarico, per effetto dell'approvazione del presente modello, al RPD sono attribuiti i seguenti poteri e prerogative:

a) **potere di autoregolamentazione**. Il RPD potrà programmare autonomamente le proprie attività, garantendo comunque l'assolvimento dei compiti precedentemente indicati e rendendo conto delle attività effettivamente espletate ai fini della verifica di idoneità ed efficace attuazione sistema privacy implementato rispetto agli obblighi di cui al GDPR; il RPD potrà farsi coadiuvare da personale appartenente alla propria Struttura organizzativa dotato di competenze specifiche nella materia, ferma restando la responsabilità finale dello stesso sugli atti ed indicazioni formalizzate;

b) **poteri ispettivi**: nell'esercizio delle proprie funzioni di controllo, il RPD potrà:
   - ✓ utilizzare le risultanze delle attività ispettive interne (ad es., verifiche di I livello dei "delegati del Titolare", audit del Sistema qualità certificato, audit tecnici su sistemi informativi, etc.) ovvero svolgere autonomamente verifiche anche a sorpresa;
   - ✓ accedere liberamente ad ogni documento rilevante per lo svolgimento delle sue funzioni;
   - ✓ disporre l'acquisizione di informazioni, dati e/o notizie a semplice richiesta, senza preventiva autorizzazione;
   - ✓ richiedere l'audizione ovvero il coinvolgimento nelle attività di verifica di qualsivoglia dipendente dell'Ente;
   - ✓ esercitare i poteri, come precedentemente esplicitato, anche nei confronti delle società in house cui partecipa Unioncamere, quando svolgano le funzioni di Responsabili esterni del trattamento (in questi casi, affianca il competente dirigente di Unioncamere).

[2] ad es., reclami, richieste di esercizio dei diritti di cui agli artt. 12 e ss. del GDPR, richieste di riesame di eventuali risposte ottenute da altri dirigenti di Unioncamere

Il RPD non potrà essere rimosso o penalizzato arbitrariamente a causa dell'esercizio delle proprie funzioni, non potendo inoltre assumere attività o compiti concorrenti che risultino in contrasto o conflitto di interesse.

Nell'esercizio dell'incarico, il RPD garantisce il vincolo di riservatezza sui dati e sulle informazioni acquisite, fermi restando gli obblighi connessi ad eventuali richieste formalizzate da Pubbliche autorità con funzioni inquirenti, giudicanti e di controllo.

I dati di contatto del RPD (recapito postale, telefono, email) sono resi disponibili sul sito internet di Unioncamere, riportati nelle informative rese agli interessati e comunicati al Garante per la protezione dei dati personali.

## DELEGATI DEL TITOLARE DEL TRATTAMENTO

Ai seguenti soggetti, ai sensi dell'art. 2-quaterdecies, co. 1 del D.Lgs. 196/2003 ed in forza dei poteri statutari e delle deleghe gestionali conferite, è assegnata, per effetto dell'approvazione del presente documento[3], la gestione delle funzioni di seguito descritte. Ove l'esercizio di tali funzioni comporti impegni di spesa non rientranti nei poteri/deleghe conferite ordinariamente, la relativa decisione sarà rimessa al Comitato esecutivo.

## IL SEGRETARIO GENERALE

Il **Segretario Generale**, in qualità di organo di vertice dell'amministrazione, sovrintende alla gestione complessiva ed all'attività amministrativa, esercita i poteri di coordinamento, verifica e controllo dell'attività dei dirigenti, vigila sull'efficienza e rendimento degli uffici e ne riferisce agli organi secondo le rispettive competenze. Adotta tutti gli atti di organizzazione riservati dalla legge all'ambito d'autonomia della dirigenza di vertice.

Coerentemente con le competenze statutarie, il SG esercita le seguenti funzioni:

a) sottoscrizione degli **accordi di co-titolarità,** su delega specifica e previa approvazione del Comitato esecutivo;
b) aggiornamento e manutenzione, con propria determinazione, dei **documenti gestionali** approvati dal Comitato Esecutivo in funzione delle modifiche normative ed organizzative eventualmente intervenute ed all'emergere di eventuali criticità o necessità di miglioramento gestionale;
c) predisposizione ed approvazione di eventuali **documenti operativi** (es., linee guida, procedure, istruzioni operative, format di informative e consensi, etc.) del sistema di gestione che si rendessero necessari per garantire la più efficace implementazione dei requisiti del GDPR;
d) **sottoscrizione delle notifiche dei data breach** ed approvazione delle comunicazioni agli interessati, secondo quanto previsto da apposita procedura gestionale;
e) gestione degli adempimenti derivanti dall'esercizio **dei diritti degli interessati** (artt. 15 e ss. del GDPR) e/o i **reclami** pervenuti direttamente alla Segreteria Generale ovvero relativi a processi o fasi di attività nella propria diretta competenza[4], provvedendo ad alimentare il "Registro delle richieste di esercizio dei diritti degli interessati"; fornisce supporto al RPD ove la richiesta sia pervenuta direttamente a lui ovvero in fase di "riesame" della risposta formalizzata all'interessato, ove richiesto;
f) **dotazione di misure di sicurezza di tipo tecnico-informatico** da applicarsi unitariamente all'Unioncamere, ovvero non rientranti nelle specifiche responsabilità e budget delle Aree Dirigenziali;
g) approvazione (previa progettazione dell'Area Organizzazione e Personale e valutazione positiva dell'RPD) di **percorsi formativi e strumenti informativi periodici**, al fine di definire necessarie istruzioni ai dirigenti, ai quadri, nonché ai soggetti che – agendo sotto l'autorità del Titolare - svolgono trattamenti nell'ambito delle Aree, Servizi ed Uffici di Unioncamere;
h) definizione e sottoscrizione – ove rientrante nelle proprie nelle proprie competenze, deleghe e poteri di spesa – delle **clausole contrattali o atti giuridici analoghi** per il conferimento delle responsabilità del trattamento a soggetti esterni (art. 28);
i) nomina individuale degli **amministratori di sistema** che agiscono su strumenti e sistemi "generali" dell'Unioncamere e la valutazione degli stessi[5], in attuazione di quanto riportato nel Disciplinare tecnico per le funzioni di amministratore di sistema;
j) gestione dei **flussi informativi** al RPD di propria competenza, come definiti nell'apposito paragrafo del presente documento, e più in generale comunicazione **allo stesso di ogni notizia rilevante** ai fini della protezione dei dati personali e degli interessati.

Svolge infine per gli uffici e le funzioni di staff nella sua afferenza diretta, le funzioni di cui al par. successivo.

[3] E mediante specifico richiamo nell'atto di conferimento dell'incarico alle funzioni previste dal presente documento; l'allocazione delle responsabilità derivanti da tale designazione è sempre verificabile, per relationem, con riferimento all'organigramma nominativo nel tempo vigente di cui alla nota 1
[4] ove non ricedenti nella specifica responsabilità *ratione materiae* di un'area dirigenziale.
[5] Come richiesta dallo specifico Provvedimento del Garante di cui al § "Amministratori di Sistema"

## I RESPONSABILI DELLE AREE DIRIGENZIALI

Alla dirigenza spetta la gestione finanziaria, tecnica e amministrativa, mediante autonomi poteri di spesa, di organizzazione delle risorse umane e strumentali, nonché di controllo. La dirigenza è responsabile della gestione e dei relativi risultati.

In coerenza con le funzioni statutarie, ai Dirigenti sono delegate le seguenti funzioni:

a) **applicano -** nel contesto della specifica mission dell'Area di riferimento **- la normativa e le istruzioni** definite dal Titolare in collaborazione con il RPD attraverso i documenti gestionali del sistema privacy; i Dirigenti sono destinatari di ogni comunicazione di carattere generale (ad es., regolamenti, procedure, circolari, linee guida, provvedimenti...) in materia di privacy da parte del Comitato Esecutivo, del SG e dell'RPD, in esecuzione delle quali dovranno provvedere a contestualizzarle in relazione allo specifico contesto produttivo di riferimento e veicolarle tempestivamente ai propri collaboratori garantendone l'applicazione[6];

b) verificano le esigenze di integrazione od aggiornamento dei documenti gestionali predisposti, ad es., evidenziando al Segretario Generale ed al RPD le eventuali **necessità di modifica/integrazione del registro dei trattamenti** di cui all'art. 30 del Regolamento, in relazione – a puro titolo esemplificativo - ad:
   - esigenze derivanti da nuovi servizi/progetti diversi o nuovi rispetto a quelli attualmente censiti;
   - modifiche organizzative interne all'Area di competenza che comportino diverse modalità di gestione dei trattamenti di dati, anche ai fini dell'analisi dei rischi (ad es., acquisizione di applicativi informatici per la gestione di determinate attività rientranti nella propria autonomia gestionale);

c) rilevano e segnalano alla competente Area le eventuali e specifiche **esigenze formative o di approfondimento** da considerare ai fini della progettazione e programmazione dei percorsi formativi interni;

d) adottano ordinariamente, ovvero in caso di criticità e problematiche sopravvenute, **tutte le misure preventive e correttive[7] a tutela dei dati personali che le competenze connesse al ruolo consentano di assumere** (rientranti nell'ambito delle funzioni e budget attribuite), rappresentando al SG ed al RPD specifiche esigenze cui non possono far fronte ordinariamente;

e) garantiscono, in relazione alle necessità di volta in volta emergenti nell'ambito dei servizi di competenza, il rilascio del**l'informativa** di cui agli artt. 13 e 14 del GDPR e l'acquisizione del **consenso** dagli interessati (ove necessario);

f) effettuano, nell'ambito delle funzioni istruttorie connesse alla proposta dei relativi atti, l'istruttoria necessaria per la definizione degli **accordi di co-titolarità** da sottoporre alla firma del Presidente o del Segretario Generale;

g) in caso di **affidamento di servizi ed incarichi professionali mediante appalto, contratti di servizi o altre tipologie contrattuali che comportino il conferimento/trattamenti di dati affidati all'esterno**:
   - in qualità di **dirigente proponente** (ovvero in collaborazione con il) **responsabile unico del procedimento** provvedono:
     - alla individuazione degli elementi di esperienza ed affidabilità che costituiscono il presupposto per l'affidamento dell'incarico di trattamento[8];
     - alla definizione degli adempimenti gestionali e tecnici che devono essere garantiti dal fornitore, in ragione della tipologia di dati e dei trattamenti da eseguire sugli stessi, da prevedere nel contratto di servizi o in atto giuridico analogo quale parte delle obbligazioni negoziali e quindi di carattere cogente;
   - in qualità di (ovvero in collaborazione con il) **Responsabile/Direttore dell'esecuzione del contratto/Referente contrattuale**, verificano il rispetto delle regole definite contrattualmente;

h) istruiscono le **richieste di esercizio dei diritti** degli interessati (artt. 15 e ss. del GDPR) e/o i **reclami** pervenuti direttamente all'Area ovvero relativi a progetti, processi o fasi di attività nella propria competenza e provvedono a formalizzare le risposte (e ad alimentare il "Registro delle richieste di esercizio dei diritti degli interessati"); le propongono al SG ove rientranti nella sua diretta responsabilità; forniscono supporto al RPD ove la richiesta sia pervenuta direttamente a lui ovvero in fase di "riesame" della risposta formalizzata all'interessato, ove richiesto;

k) gestiscono – secondo quanto definito da apposita procedura gestionale - il coordinamento del processo di analisi, gestione e risposta alle violazioni di dati verificatesi in relazioni a processi, progetti, basi di dati rientranti nella propria specifica responsabilità o competenza; acquisiscono gli elementi informativi utili a valutare la necessità/obbligo di notifica dei **data breach** al Garante ed agli interessati, compresa l'alimentazione del "Registro dei Data breach";

---

[6] Ad es., personalizzazione dei format e modelli per la gestione degli adempimenti in relazione alle necessità di volta in volta emergenti nell'ambito della propria attività

[7] connesse ad es., all'organizzazione interna del lavoro, alla gestione di eventuali fornitori e strumenti informatici, ai flussi informativi e documentali di competenza, etc.

[8] "Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato", art. 28, par. 1 del GDPR

i) garantiscono che la **diffusione** dei dati personali (diversi da quelli sensibili e giudiziari che risulta allo stato essere vietata) avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero solo se prevista da specifica normativa (ad es., con riferimento agli obblighi di pubblicazione per finalità di pubblicità integrativa dell'efficacia e di trasparenza (ai sensi del D.Lgs. 33/2013 e s.m.i.) per quanto di competenza;
j) si attivano - in collaborazione con il RPD - per fare in modo che, in relazione ad **ogni nuova iniziativa o progetto** che comporti un trattamento di dati personali, sia effettuata **una verifica preventiva della liceità e della legittimità del trattamento,** nonché delle modalità con le quali si intende eseguirlo; ove necessario, sulla base degli artt. 35 e 36 del Regolamento e delle Linee guida WP29 e del Garante, provvedono ad eseguire, in collaborazione con il RPD, la **valutazione d'impatto sulla protezione dei dati** e supportare il Presidente nell'attivazione della **consultazione preventiva** del Garante ove ritenuta necessaria;
k) formalizzano la nomina individuale degli **amministratori di sistema** che agiscono su strumenti e sistemi "verticali" utilizzati nell'ambito delle competenze della propria Area e la valutazione degli stessi[9], in attuazione di quanto riportato nel Disciplinare tecnico per le funzioni di amministratore di sistema;
l) gestiscono i **flussi informativi** al RPD di propria competenza, come definiti nell'apposito paragrafo del presente documento, e più in generale comunicano **allo stesso di ogni notizia rilevante** ai fini della protezione dei dati personali e degli interessati.

## SOGGETTI AUTORIZZATI AL TRATTAMENTO

In merito è da puntualizzare che, pur non prevista espressamente dal Regolamento quale qualifica soggettiva, il D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018 ha lasciato ampia scelta al Titolare del trattamento nel definire le modalità ritenute più idonee per autorizzare al trattamento i soggetti che operano sotto la propria autorità diretta.

Unioncamere in merito ritiene di dover mantenere le modalità gestionali precedentemente utilizzare per la designazione degli "incaricati del trattamento"; quindi i soggetti che svolgono trattamenti "per conto" del Titolare sono **formalmente autorizzati:**

a) **"*per relationem*" ove dipendenti,** all'atto dell'assegnazione/allocazione (anche temporanea, con ordini di servizio successivi) in un centro di responsabilità (Area/Servizio/Ufficio) per il quale sia definito per iscritto l'ambito del trattamento (mediante rinvio al registro dei trattamenti ed alle istruzioni impartite);
b) per i **collaboratori esterni e consulenti/professionisti** (ove nel concreto operanti sotto l'autorità diretta del Titolare[10]) mediante previsione di idonee clausole contrattuali in riferimento ai trattamenti oggetto dell'incarico stesso, contenenti le eventuali istruzioni specifiche necessarie per l'esecuzione delle attività previste.

Il personale autorizzato deve effettuare le operazioni di trattamento secondo le **istruzioni impartite dal Titolare anche per il tramite dei soggetti di cui ai paragrafi precedenti**, e rimane soggetto al potere di vigilanza e controllo di questi ultimi. Nello specifico, i soggetti autorizzati dovranno:

- ✓ garantire la massima **riservatezza** su qualsiasi informazione e dato personale di cui vengano a conoscenza nell'esercizio delle proprie funzioni, in conformità a quanto previsto normativamente in tema di **segreto d'ufficio** e di **segreto d'impresa**;
- ✓ fare riferimento alla specifica scheda analitica del registro dei trattamenti per l'individuazione **degli elementi fondamentali dei trattamenti** che si è autorizzati ad effettuare;
- ✓ seguire obbligatoriamente i **percorsi formativi** che saranno organizzati dall'Ente;
- ✓ rispettare le **disposizioni impartite per iscritto** dal Titolare o dal Delegato del Titolare competente attraverso la documentazione rilevante a fini privacy, nonché tutte le ulteriori istruzioni che possono essere formalizzate dai soggetti di cui ai par. precedenti;
- ✓ utilizzare le **misure di sicurezza** per la protezione fisica, informatica e telematica dei dati personali secondo le specifiche istruzioni definite nell'ambito del sistema di gestione privacy e dal Regolamento per l'utilizzo degli strumenti informatici e delle misure di sicurezza;
- ✓ **comunicare al RPD**, attraverso il Delegato, **ogni notizia rilevante** ai fini della protezione dei dati personali e degli interessati; qualora ne venga a conoscenza nell'espletamento delle attività di competenza o indirettamente nello svolgimento delle stesse, **informare** tempestivamente (possibilmente entro il limite di 24 ore dal momento in cui si viene a conoscenza del fatto) **il RPD**, attraverso il Delegato/Referente privacy, del **verificarsi di eventuali violazioni dei dati personali** che possano esporre a rischio le libertà ed i diritti degli interessati ovvero la sicurezza, integrità e disponibilità dei dati trattati **(data breach**);
- ✓ **collaborare più in generale con il RPD** provvedendo a fornire ogni informazione da questi richiesta.

[9] Come richiesta dallo specifico Provvedimento del Garante di cui al § "Amministratori di Sistema".
[10] Come meglio specificato in apposite Linee guida del Sistema di Gestione dei Dati Personali di UC

Il soggetto autorizzato potrà fare riferimento direttamente al RPD per l'**esercizio dei diritti** che gli sono propri in qualità di interessato al trattamento dei propri dati personali (artt. 15 e ss. del GDPR).

### AMMINISTRATORI DI SISTEMA

Il Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e s.m.i. definisce l'amministratore di sistema come la «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».

I soggetti che svolgono funzioni di amministrazione di sistemi (ad es., addetti alla gestione e manutenzione di un impianto di elaborazione o di sue componenti; amministratori di basi di dati; amministratori di reti e di apparati di sicurezza, amministratori di applicativi complessi):

- ✓ sono "responsabili" di specifiche fasi lavorative ovvero di strumenti che possono comportare elevate criticità rispetto alla protezione dei dati;
- ✓ pur non essendovi preposti istituzionalmente, possono anche "solo incidentalmente" trovarsi nella necessità di trattare dati personali ai soli fini dell'espletamento delle loro consuete attività.

Il Provvedimento del Garante definisce gli **adempimenti da formalizzare** sia in relazione ai dipendenti che svolgano tali funzioni sia nel caso di servizi affidati in outsourcing.

In attuazione di tale provvedimento, Unioncamere:

**a)** ha adottato uno **specifico documento del proprio sistema di gestione privacy** al fine di:
- ✓ instaurare il **regime di conoscibilità** dell'identità degli amministratori di sistema quale forma di trasparenza interna a tutela dei lavoratori, nel caso in cui tali figure trattino anche dati personali riferiti a questi ultimi; tale adempimento è gestito anche attraverso la specifica informativa rivolta ai dipendenti e collaboratori;
- ✓ definire **specifiche cautele** nello svolgimento delle mansioni svolte, unitamente ad accorgimenti e misure, tecniche e organizzative volte ad agevolare l'esercizio dei **doveri di controllo** da parte del Titolare (*due diligence*) previste dal citato Provvedimento;

**b)** provvede alla **designazione degli stessi**:
- ✓ nell'ambito della designazione a responsabile esterno del trattamento (art. 28 del GDPR) per i fornitori di servizi, attribuendo al soggetto esterno specifici compiti ed istruzioni;
- ✓ con atto individuale (per gli amministratori di sistema persone fisiche, a qualunque titolo impiegate: dipendenti, collaboratori e professionisti).

Nel citato documento si è disciplinato nel dettaglio:

- l'individuazione degli amministratori di sistema (interni ed esterni) e dei compiti e responsabilità loro assegnati;
- le istruzioni tecniche o impartite a tali figure nell'espletamento dei loro compiti istituzionali;
- le modalità e procedure che consentono al Titolare del trattamento di verificare l'attività svolta in relazione alle istruzioni impartite.

## FORMAZIONE ED INFORMAZIONE INTERNA

Nell'ottica di diffondere le conoscenze relative alla materia e di fornire adeguate istruzioni a tutto il personale Di Unioncamere:

- tutta la documentazione relativa al Sistema di Gestione della Privacy è resa disponibile mediante condivisione in apposita cartella della intranet ovvero con forme equivalenti;
- il funzionamento del Sistema di Gestione è presentato e descritto a tutti i Delegati del Titolare in specifici incontri di condivisione, al fine di agevolarne la conoscenza e lo svolgimento dei ruoli e delle attività previste;
- realizza progetti formativi specifici:
  - per i dipendenti che dovranno coadiuvare i Delegati del Titolare per gli adempimenti di propria competenza, ferme restando le relative responsabilità in capo ai questi ultimi;
  - i dipendenti che dovranno svolgere, nell'ambito delle Aree di appartenenza, attività di amministratore di sistemi;
  - per i dipendenti che potranno svolgere, per periodi limitati, nell'ambito dei servizi di Unioncamere al sistema camerale, attività di Responsabile per la protezione dei dati. In questi casi la formazione, di tipo permanente, avrà natura qualificante;

- è prevista, nel primo periodo di implementazione del presente modello e secondo le esigenze rappresentate dai Delegati, la progettazione e realizzazione di un piano formativo per tutti i soggetti autorizzati al trattamento; tale percorso potrà essere realizzato, al fine di raggiungere più facilmente tutti gli interlocutori e contenere i costi di realizzazione, anche in forma di e-learning

Potranno inoltre essere pianificati ulteriori specifici percorsi od eventi secondo le modalità ritenute più idonee (seminari, workshop, convention, incontri frontali…), nei quali si terrà conto anche delle specifiche esigenze comunicate dai delegati del Titolare.

L'organizzazione di tali percorsi ed eventuali specifiche azioni formative

- ✓ saranno progettati e gestiti operativamente dal Dirigente dell'Area Organizzazione e Risorse Umane, in accordo con il SG ed il RPD;
- ✓ saranno monitorate sia per quanto riguarda la realizzazione che gli esiti dal RPD.

I dipendenti e collaboratori di Unioncamere potranno inoltre fare riferimento direttamente al RPD (attraverso la specifica casella di posta elettronica: rpd-privacy@unioncamere.it) per la proposta di quesiti, la richiesta di approfondimenti etc.

Ulteriori attività di formazione/informazione saranno programmate al momento dell'assunzione di nuove risorse, nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento di dati personali.

## STRUMENTI PER IL MONITORAGGIO E CONTROLLO DEL SISTEMA

### REGISTRAZIONI, DOCUMENTAZIONE E FLUSSI INFORMATIVI

L'attuazione di un sistema di **monitoraggio, verifica e controllo** del sistema privacy implementato rispetto alla normativa ed alle direttive ed istruzioni impartite è una specifica responsabilità del Titolare del trattamento, rientrante negli obblighi di accountability di cui agli artt. 24[11] e 32 del GDPR[12].

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

- ❖ controllo di I livello (c.d. "controllo di linea"), posto in essere dai dirigenti ("delegati del Titolare") nell'ambito delle ordinarie funzioni di coordinamento e gestione delle attività di propria competenza;
- ❖ controllo di II livello (c.d. "controllo di compliance") affidato al RPD come descritto nell'apposito paragrafo del presente documento.

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

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

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

La tenuta dei Registri è affidata al RPD, l'alimentazione degli stessi è regolamentata da apposite istruzioni/procedure del Sistema di Gestione dei Dati Personali e garantita dai seguenti flussi informativi.

I format dei Registri sono riportati in Allegato ai rispettivi documenti cui si riferiscono.

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

---

[11] "… il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario".

[12] "… il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso… d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".

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

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

| PERIODICITÀ | DESCRIZIONE FLUSSO INFORMATIVO | RESPONSABILE FLUSSO |
|---|---|---|
| Tempestiva | Copia delle richieste di informazioni da parte di organi di Polizia Giudiziaria (ad es., Carabinieri, Polizia, Guardia di Finanza, etc.) o dal Garante e di tutti i verbali di accesso e di contestazione a seguito di ispezioni e controlli | Segretario Generale |
| Tempestiva | Sanzioni comminate da Pubbliche autorità in materia di privacy | Segretario Generale |
| Tempestiva | Copia dei verbali degli audit di I parte e dell'Ente di certificazione (ISO 9001) in cui si evidenzino criticità lato privacy | RSGQ |
| Quadrimestrale | Schede di rilevazione eventi (cfr. procedura data breach) | Delegati del Titolare |
| Quadrimestrale | Verbali di analisi degli incidenti (cfr. procedura di data breach) | Delegati del Titolare |
| Quadrimestrale | Risposte agli interessati in caso di reclami/esercizio diritti | Delegati del Titolare |
| Tempestiva | Informativa relativa al rifiuto di assunzione del ruolo/designazione a Responsabile esterno del trattamento | Delegati del Titolare |

## INDICATORI DI ANOMALIA DEL SISTEMA PRIVACY

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

| DIMENSIONE DEL MONITORAGGIO | DESCRIZIONE INDICATORE | VALORE SEGNALETICO | FONTE DI REPERIMENTO DEL DATO |
|---|---|---|---|
| COMPLIANCE ALLA NORMATIVA | Numero di richieste di esercizio dei diritti ex artt. 15 e ss. del GDPR o di reclami pervenuti dagli interessati nell'anno | > 5 | Registro delle richieste di esercizio dei diritti |
| | Numero di richieste/reclami con identico oggetto o relative ad uno stesso trattamento | > 3 | |
| | Tempi di risposta alle richieste di esercizio dei diritti da parte degli interessati | ≤ 30 gg | |
| | Numero di ispezioni subite da pubbliche autorità su segnalazione/denuncia degli interessati nell'anno | > 1 | Flussi informativi al RPD |
| | Numero di sanzioni comminate in materia da pubbliche autorità nell'anno | > 0 | |
| | Numero di soggetti esterni che hanno rifiutato la designazione a Responsabile esterno del trattamento | > 2 | |
| | | | |
| | | | |
| CONTROLLO E MIGLIORAMENTO CONTINUO | Numero di privacy audit effettuati nell'anno | ≤ 1 | Verbali di audit/ Relazioni agli Organi |
| | % di Non Conformità (NC) riscontrate (n. NC / n. audit) | ≥ 20% | |
| | Numero relazioni del RPD agli Organi | < 1 | Relazioni agli Organi |
| | | | |

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

### PRIVACY AUDIT

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

Il RPD potrà essere affiancato da personale appartenente alla propria Struttura organizzativa dotato di competenze specifiche nella materia ovvero da professionisti e consulenti di propria fiducia. Ove se ne ravvisi l'esigenza (ad es., ove l'Area sottoposta a verifica sia quella di cui il RPD è dirigente responsabile), anche al fine di garantire la "**separation of duty**", le verifiche potranno essere condotte da soggetti esterni qualificati ed indipendenti, secondo gli standard definiti dalla norma UNI EN ISO 19011:2012 ""Linee guida per audit di sistemi di gestione".

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

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

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

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

## RIESAME ED AGGIORNAMENTO DEL SISTEMA DI GESTIONE DELLA PRIVACY

Nell'ottica del miglioramento continuo e del raggiungimento degli obiettivi di compliance alla normativa di riferimento, anche al fine di garantire che l'efficacia delle misure tecniche e organizzative implementate sia "testata regolarmente" (art. 32, par. 1, lett. d), il Comitato Esecutivo esegue almeno annualmente un **riesame del Sistema di gestione della Privacy** con lo scopo di:

a) valutare il grado di attuazione del Sistema;
b) verificare la sua efficacia ed idoneità rispetto alle specifiche esigenze di compliance;
c) individuare specifiche azioni correttive e preventive da intraprendere, nonché elementi conoscitivi utili al miglioramento dello stesso.

Il riesame deve essere sempre condotto, inoltre, in occasione:

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

Il riesame è istruito preliminarmente in forma di relazione periodica dal RPD, tenuto conto delle informazioni disponibili quali desunte dalle proprie attività di supporto e di controllo. La Relazione è inviata almeno 10 giorni prima della riunione del Comitato Esecutivo e presentata dal RPD in tale sede, per l'assunzione delle eventuali decisioni necessarie per garantire la compliance ed il miglioramento continuo.

ALLEGATO 2

UNIONCAMERE

# SGDP - SISTEMA DI GESTIONE DEI DATI PERSONALI
# Linee guida per l'allocazione delle responsabilità a soggetti esterni

ai sensi del Regolamento UE 679/2016

## SOMMARIO

# PREMESSA

## SCOPO E CAMPO DI APPLICAZIONE

Scopo della presente linea guida è di definire il set di adempimenti, relative responsabilità e strumentazione operativa per la valutazione di soggetti esterni in rapporti contrattuali/convenzionali con Unioncamere e l'allocazione delle responsabilità per il trattamento dei dati, in qualità di Contitolari o Responsabili.

In proposito, si specifica che non tutti i contratti con soggetti esterni cui sono affidate attività o servizi di competenza di Unioncamere comportano l'attivazione di specifiche cautele a tutela dei dati e degli interessati. Ciò è vero innanzitutto nel caso in cui l'affidamento **non comporti il trattamento di dati personali**; in tali casistiche – la cui verifica compete al soggetto che esprime e qualifica il fabbisogno di beni, servizi o lavori - non dovrà essere gestito alcun adempimento di cui al presente documento.
La presente linea guida è portata a conoscenza, anche attraverso attività di sensibilizzazione o formazione, di tutti i Dirigenti, Quadri, funzionari o, comunque, referenti delle Aree/Uffici di Unioncamere potenzialmente coinvolti nella stessa.

## RIFERIMENTI NORMATIVI

La presente procedura risponde ai seguenti requisiti normativi:

1. Contitolare del trattamento (art. 4, n. 7 e art. 26 del GDPR);
2. Responsabile del trattamento (art. 4, n. 8 e art. 28 del GDPR);
3. Amministratori di sistema (Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e s.m.i.);
4. WP29, Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento".

## ACRONIMI E DEFINIZIONI UTILIZZATE

| | |
|---|---|
| GDPR | Regolamento UE 2016/679 (General Data Protection Regulation) |
| Codice | D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. 101/2018 |
| Garante | Garante per la protezione dei dati personali |
| RPD | Responsabile della protezione dei dati |
| Delegato del Titolare | Soggetto che, secondo le deleghe/procure formalizzate ed il sistema di gestione della privacy, garantisce specifiche funzioni ai fini della *compliance* al GDPR |
| SG | Segretario Generale di Unioncamere |
| Responsabile | Responsabile del trattamento ex art. 28 GDPR |
| | |
| | |
| | |
| | |

## MATRICE DELLA REDAZIONE E DELLE REVISIONI

| Data | Stato | Descrizione | Approvazione |
|---|---|---|---|
| 13/12/2018 | Approvato | Rev 0 – I[a] emissione | Delibera del Comitato esecutivo del 13/12/2018 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## CONTITOLARITÀ

Due soggetti possono assumere la qualifica di **Contitolari** ai sensi degli artt. 4, par. 1, n. 7 e art. 26 del GDPR, quando, in relazione ed uno o più trattamenti, determinino **congiuntamente le finalità e i mezzi** dello stesso. A tali fini:

- per "finalità" deve intendersi il "perché" debba essere effettuato un trattamento di dati;
- per "mezzi", devono intendersi non solo gli strumenti tecnici utilizzati per trattare i dati personali (ad es., uno specifico applicativo informatico e le relative misure di sicurezza), ma anche il "come" del trattamento, cioè "quali dati trattare", "chi può avervi accesso", "quanto tempo conservarli ", ecc.

In proposito, si specifica che la qualifica di Titolari del trattamento è desumibile:

a) in forza di una Legge o disposizione di fonte secondaria[1] (c.d. "**esplicita competenza giuridica**") che attribuiscano istituzionalmente ad Unioncamere una "funzione istituzionale" (cfr. l'art. 7 della legge n. 580/1993);
b) in forza di un **contratto o atto analogo tra le parti** che consentano esplicitamente od implicitamente (ovvero per *facta concludentia*[2]) di assegnare ad una od entrambe le parti tale qualifica;
c) a prescindere da una specifica competenza o facoltà di controllare dati conferita per legge o per contratto, sulla base di elementi fattuali e circostanze concrete (c.d. "**competenza implicita**") che pongano l'Ente od Organizzazione in una "posizione di dominanza" rispetto ai dati acquisiti, ovvero eserciti "in autonomia" un determinato trattamento.

Si possono ipotizzare, in proposito, alcuni esempi di contitolarità riferibili ad Unioncamere, da valutare sempre caso per caso e nello specifico contesto:

1. Unioncamere ed altra Pubblica Amministrazione centrale si accordano (mediante la stipula di un protocollo, convenzione o atto giuridico analogo) per svolgere una determinata attività o progetto che comporti il trattamento di dati personali (in funzione delle circostanze, i due Enti possono essere entrambi competenti *ratione materiae* in riferimento all'oggetto dell'accordo, ovvero la competenza può essere derivata direttamente dallo strumento contrattuale);
2. Unioncamere assume un ruolo di garanzia/controllo su una determinata tematica/attività (es., in qualità di Organismi direttivi centrali), nell'ambito dell'attuazione di Convenzioni internazionali;
3. Unioncamere partecipa in partnership con altri Enti e Società del Sistema camerale o con Organizzazioni esterne ad esso a Programmi nazionali o comunitari per il finanziamento di specifiche progettualità che comportano l'acquisizione e gestione di dati personali;
4. Nell'ambito delle funzioni attribuite agli Enti del Sistema camerale dalla Legge 580/1993 e s.m.i., Unioncamere e le Camere di Commercio pongono in essere progettualità o servizi gestiti congiuntamente.

La verifica della possibile situazione di contitolarità – prima dell'approvazione del relativo documento da parte dell'organo competente - deve essere effettuata dal Segretario Generale o dal Dirigente dell'Area organizzativa di riferimento proponente l'atto convenzionale o la specifica progettualità, in collaborazione con la controparte contrattuale; in questi casi deve essere attivato, nella fase istruttoria, il RPD che può formalizzare uno specifico parere in proposito o collaborare alla fase istruttoria.
In caso di esito positivo, sulla base delle competenze in merito alla procedura, si provvederà ad includere nello stesso atto convenzionale (o in specifico accordo interno stipulato *a latere* dell'atto principale) la definizione delle responsabilità delle parti in merito all'osservanza degli obblighi derivanti dal Regolamento, con specifico (ma non esclusivo) riferimento:

- all'identificazione del soggetto che rilascia l'informativa ed acquisisce gli eventuali consensi al trattamento e che risponde in caso di esercizio dei diritti da parte degli interessati;
- l'eventuale previsione di un unico punto di contatto (es., Responsabile per la Protezione dei Dati) per gli interessati.

Qualora dall'istruttoria effettuata vi sia l'ipotesi di:

a) avvio di un nuovo trattamento (non precedentemente effettuato da nessuno dei due o più partner);
b) oppure utilizzo (anche su trattamenti già effettuati) di nuove tecnologie;
c) e tali situazioni è probabile che presentino un rischio elevato per i diritti e le libertà delle persone fisiche, secondo quanto previsto da apposite linee guida in materia di Data Protection Impact Assessment del SGDP di Unioncamere.

L'atto convenzionale (o accordo interno) deve inoltre prevedere:

[1] Ad es., decreti ministeriali
[2] In relazione ad es., al grado di controllo reale esercitato da una parte, all'immagine complessiva data agli interessati ed il conseguente legittimo affidamento di questi ultimi sul soggetto che – in base a questa immagine – anche solo appaia esercitare il controllo sui dati

- il soggetto che effettua la DPIA (Data Protection Impact Assessment) di cui all'art. 35 del GDPR[3] e, in caso di necessità, la consultazione preventiva dell'Autorità Garante (art. 36 del GDPR).
- il soggetto che, in relazione alla responsabilità come ripartite nell'atto convenzionale o accordo, dovrà tenere in considerazione le risultanze della DPIA o della consultazione dell'Autorità di controllo ai fini dell'implementazione di adeguate misure a tutela degli interessati.

Nel caso in cui dall'accordo istituzionale prenda avvio una specifica progettualità comprendente lo sviluppo di strumenti/applicativi informativi, portali informativi o gestionali o strumenti simili, devono essere definite le responsabilità relative alle fasi di progettazione funzionale e non funzionale (misure di sicurezza) dello stesso, in ossequio ai principi della privacy by design & by default, e la gestione dello stesso.

Va riservata molta attenzione alla differenza che intercorre tra la "gestione" della privacy nell'ambito dell'accordo/contratto/convenzione etc. e quelle che sono poi le attività "operative" dei "prodotti/servizi" oggetto dei citati atti. Il caso tipico è un accordo che prevede la creazione/gestione di un portale web.

Di seguito si riporta una bozza di accordo di contitolarità:

**UNIONCAMERE – UNIONE DELLE CAMERE DI COMMERCIO D'ITALIA** con sede legale in Piazza Sallustio, 21 - 00187 Roma; Tel.: 06.47041 - Fax: 06.4704240 - PEC: unioncamere@cert.legalmail in persona del _____ *qualifica*_____, _____*nome*_____, che agisce in qualità di soggetto delegato ad acta dal Titolare del trattamento

e il **CONTRAENTE** _____, in persona del _____ *qualifica*_____, _____*nome*_____, che agisce in qualità di soggetto delegato ad acta dal Titolare del trattamento

d'ora in poi anche congiuntamente denominate le '**Parti**', ai sensi e per gli effetti dell'art. 4 n. 7 e dell'art. 26 del Regolamento UE 679/2016, convengono e stipulano quanto segue:

**Art. 1. Oggetto.**
L'oggetto del presente accordo è l'instaurazione di un rapporto di contitolarità tra le Parti per il trattamento dei dati acquisiti, gestiti e trattati ai fini della realizzazione _____ *descrivere l'oggetto e la finalità delle attività previste dall'accordo, nonché la base legale su cui l'attività è posta in essere* _____.
L'attività di cui trattasi comporterà il trattamento di dati _____ *qualificare i dati personali acquisiti* _____, relativi a _____ *qualificare tipologia di interessati* _____

**Art. 2. Ripartizione delle responsabilità**
Le Parti, come in effetti con il presente accordo pongono in essere, intendono trattare i dati acquisiti e gestiti, stante le medesime finalità e modalità del trattamento definite in sede progettuale, in regime di contitolarità, e per ragioni di sinergia, di condivisione delle strutture, delle risorse come di seguito delineato:

| UNIONCAMERE | CONTRAENTE |
|---|---|
| | |
| | |
| | |
| | |

*Descrivere in tabella le tipologie di trattamento posto in essere singolarmente o congiuntamente dalle parti, comprese le finalità, scomponendo in processi, sotto-processi e fasi di trattamento ove opportuno al fine di circoscrivere le responsabilità a quanto effettivamente realizzato*

Rimane fermo che le Parti sono vincolate all'utilizzo dei dati secondo le finalità definite in ambito progettuale e qui richiamate nonché esposte nelle informative rilasciate agli interessati, che dovranno comunque prevedere il contenuto essenziale del presente accordo.

[3] Per l'identificazione delle casistiche in cui è necessario o consigliabile effettuare la DPIA nonché dei parametri da utilizzare per la realizzazione della stessa si faccia riferimento al documento *WP248 - 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 04/10/2017, reperibile al seguente link: https://www.garanteprivacy.it/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati

**Art. 3. Dati**
La "contitolarità" è riferita alla acquisizione congiunta e/o disgiunta e/o al conseguente trattamento dei dati acquisiti dalle Parti per le finalità sopra riportate, intendendosi per "trattamento" qualunque operazione o complesso di operazioni effettuate con o senza l'ausilio di strumenti elettronici e concernenti la raccolta, la registrazione, l'organizzazione, l'archiviazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, l'utilizzo, la diffusione, la cancellazione e la distruzione di dati acquisiti ed, in definitiva, tutti i processi di gestione dei dati cui il presente accordo è riferito.

**Art. 4. Obblighi ed attività derivanti dalla contitolarità**
Nello specifico i Contitolari si assumono vicendevolmente le seguenti responsabilità:

| UNIONCAMERE | CONTRAENTE |
|---|---|
| | |
| | |
| | |

*Definire le responsabilità connesse ad es., al rilascio dell'informativa/acquisizione del consenso (se occorre previa condivisione tra le parti), all'adozione di specifiche misure di sicurezza, ai tempi di conservazione dei dati, alla possibilità di designazione di responsabili/sub-responsabili del trattamento (se occorre previa condivisione tra le parti)*

Ai sensi dell' art. 26, par. 3 del Regolamento citato ed in relazione all'esercizio dei diritti degli interessati, questi potranno fare riferimento a ciascuno dei contitolari; al fine di agevolare tali soggetti, è definito quale punto unico di contatto: _____ *inserire contatti del punto unico di contatto, che risponderà agli interessati per conto delle due parti* _____ *(eventuale)* che dovrà essere esposto in tutte le informative rese all'esterno. In proposito, le Parti si impegnano comunque – ove la richiesta pervenga a soggetto diverso da quello cui compete l'attività di trattamento oggetto della richiesta stessa, secondo le responsabilità definite all'art. 2 – ad inoltrare immediatamente la richiesta al soggetto competente ed a supportarlo in tutto l'iter istruttorio della stessa.

In relazione all'adozione delle misure di organizzativo-gestionali e tecniche (previste o meno nell'ambito del presente accordo) ed alla gestione di eventuali violazioni, le Parti convengono che:

a) ciascuna, per i dati nella propria diretta disponibilità, è responsabile dell'adozione di misure di sicurezza adeguate (art. 32 del GDPR)
b) ciascuna si impegna a gestire gli eventuali adempimenti connessi al data breach di cui agli artt. 33 e 34 del GDPR ove riguardino attività nella propria diretta responsabilità secondo quanto stabilito all'art. 2, previa opportuna comunicazione alle altre Parti ove la violazione e la successiva notifica possa comportare anche solo un danno reputazionale agli altri Soggetti coinvolti; in merito le parti si impegnano alla massima collaborazione al fine di mitigare gli eventuali impatti derivanti dalle violazioni sui diritti e libertà degli interessati

Letto, approvato e sottoscritto tra le Parti.

## RESPONSABILI ESTERNI DEL TRATTAMENTO

Vi sono situazioni in cui Unioncamere, esternalizzando un servizio, si trova a dover consentire ad un Soggetto terzo (ovvero diverso dall'interessato e dal Titolare e relativa struttura organizzativa) di accedere ai dati personali necessari per espletarlo.

Per evitare che si rientri in una fattispecie di *comunicazione* di dati personali, in questi casi deve essere applicato lo schema di responsabilità ex art. 28 del GDPR: in buona sostanza, il soggetto esterno entra sostanzialmente a far parte del sistema privacy del Titolare (ovvero del suo ambito di titolarità, operando sotto la sua autorità); tale configurazione del rapporto legittima il terzo ad utilizzare, per la parte di competenza, i dati che rientrano nel dominio del Titolare, vincolandolo però a standard prestazionali e di comportamento ben definiti. Al responsabile esterno è riservata una parziale autonomia riguardante la sola concreta disciplina del servizio ed alcune scelte tecnico-operative, ma non anche le principali decisioni sulle finalità e sulle modalità di utilizzazione dei dati che spettano esclusivamente al Titolare del trattamento; il responsabile esterno risponderà dell'attività di trattamento in termini di corretto adempimento delle prestazioni ai sensi degli art. 1218 e 1223 del Codice Civile. Parimenti il Titolare gestirà – mediante la relazione contrattuale connessa all'incarico – i dati personali del soggetto incaricato delle attività di Responsabile esterno.

Il presupposto per l'affidamento di trattamenti a soggetti esterni, è che sia valutata nella fase istruttoria (ad es., mediante specifica previsione dei capitolati tecnici, o altrimenti mediante acquisizione di specifica documentazione della controparte) l'affidabilità del soggetto – in relazione all'esperienza, capacità, alle misure di sicurezza organizzative e tecnico-informatiche – affinché fornisca idonea garanzia del pieno rispetto delle disposizioni di cui al Regolamento UE 679/2016[4].

Elementi utili a tale verifica possono essere, a puro titolo esemplificativo:

- con riferimento ai requisiti di **capacità morale e di affidabilità**, l'assenza di condanne rilevanti in materia, ad es., con riferimento:
  - ✓ ad uno o più dei reati precedentemente previsti dal D.Lgs. 196/2003 (artt. 167 e ss.) o dall'art. 24 bis del D.Lgs. 231/2001 in relazione agli apicali dell'Ente o direttamente in capo all'Ente (sanzioni amministrative dipendenti da reato);
  - ✓ alle sanzioni amministrative in capo al Titolare del trattamento precedentemente previste dal D.Lgs. 196/2003 (cfr. artt. 161 e ss.) o successivamente dal GDPR (art. 83);
- con riferimento ai requisiti speciali (**capacità tecnica**):
  - ✓ il possesso di sistemi certificati di gestione della sicurezza delle informazioni (es., ISO 27001), di continuità operativa (es., ISO 22301) ovvero la dichiarata adesione a Linee guida o Codici di condotta specifici (es., ISO 17799, ISO/IEC 27032, Codici di condotta specifici[5]), in attesa di analoghi strumenti definiti ai sensi degli artt. 40 e ss. del Regolamento UE 679/2016;
  - ✓ l'attestazione di adozione dei controlli di natura tecnologica, organizzativa e procedurale definiti dalla Circolare AgID n. 2 del 18 aprile 2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni" (G.U. - Serie Generale n. 103 del 5 maggio 2017), a partire dal livello minimo (per la generalità dei casi, mentre i livelli superiori – Standard ed Alto – potrebbero essere utilizzati nei casi di trattamenti maggiormente impattanti);
  - ✓ *idonea e documentata attestazione e descrizione delle misure di accountability adottate ai sensi del GDPR* (ad es., registro dei trattamenti, nomina RPD) e delle misure di sicurezza organizzative e tecniche implementate ai sensi degli artt. 24 e 32 del Regolamento UE.

**Le specifiche per la valutazione del soggetto esterno sono definite – in funzione della "criticità" delle attività da affidare - dal RUP ed oggetto di valutazione da parte del RUP stesso in caso di affidamento diretto, dalla Commissione di aggiudicazione, nel caso in cui sia prevista, dal Dirigente proponente l'eventuale atto deliberativo che formalizza gli accordi convenzionali in assenza di evidenza pubblica.**

[4] Cfr. considerando 81 del GDPR: "…quando affida delle attività di trattamento a un responsabile del trattamento il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento"

[5] Ad es., Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici (Provvedimento del Garante n. 2 del 16 giugno 2004, in G.U. 14 agosto 2004, n. 190), Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (Provvedimento del Garante n. 13 del 31 luglio 2002, in G.U. 1 ottobre 2002, n. 230, come successivamente modificato dal Provvedimento del 12 giugno 2014, in G.U. n. 170 del 24 luglio 2014).

NB: ove l'appalto o l'incarico preveda lo sviluppo di applicativi informatici, portali web e strumenti analoghi, l'applicazione dei principi di privacy by design o di default prevede che debbano essere chiaramente definite, in relazione alla "consistenza" dei trattamenti e degli strumenti da implementare, nell'ambito del capitolato tecnico ovvero in documento progettuale successivo, le **specifiche non funzionali** (misure di sicurezza) da implementare, sulla base di una preliminare o successiva analisi d'impatto che dovrà costituire specifico dato di input per la realizzazione delle attività. L'identificazione delle soluzioni da ritenere adeguate (specifiche non funzionali) può anche essere rimessa al soggetto esterno (ad es., mediante richiesta di un documento di progettazione preliminare) ma in questo caso devono comunque essere sottoposte a validazione da parte del Titolare committente.

Gli stessi soggetti precedentemente identificati verificano che nel successivo contratto, convenzione o atto giuridico analogo[6] che comporti un trattamento di dati effettuato "per conto" di Unioncamere, sia personalizzata ed inserita la seguente clausola contrattuale.

ART. XY NOMINA/DESIGNAZIONE A RESPONSABILE ESTERNO DEL TRATTAMENTO AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 679/2016

Posto che la realizzazione dell'attività di cui in premessa comporta il trattamento di dati personali _____ relativi alle seguenti categorie di interessati _____, [7]in relazione ai quali Unioncamere è Titolare del trattamento ai sensi dell'art. 4, n. 7 del Regolamento UE 679/2016 (di seguito anche GDPR), si conviene quanto segue.
Il contraente, nell'esecuzione delle attività affidate, opererà in qualità di responsabile del trattamento ai sensi dell'art. 28, par. 1 del GDPR, impegnandosi a garantire la riservatezza dei dati personali degli interessati, che saranno affidati da Unioncamere e/o autonomamente acquisiti durante l'intero processo di erogazione del servizio e a non comunicarli e/o diffonderli presso terzi. Con apposito allegato al presente contratto/convenzione, la cui sottoscrizione sarà condizione di efficacia delle obbligazioni contrattuali di cui al presente documento, potranno essere indicate le specifiche istruzioni cui il contraente dovrà attenersi.
La durata del trattamento coincide con la durata contrattuale di cui all'art. __ del presente documento, fatte salve eventuali proroghe o rinnovi. La finalità del trattamento di cui al presente articolo è esplicitata nell'art. ____ (oggetto del servizio).
In caso di violazione totale o parziale della normativa vigente (Regolamento UE, D.Lgs. 196/2003 e s.m.i.) o delle istruzioni impartite mediante il citato allegato, il contraente sarà soggetto a contestazione da parte di Unioncamere che determinerà l'interruzione dei termini di pagamento. In tal caso, il contraente dovrà produrre, entro e non oltre 7 giorni lavorativi successivi alla suddetta contestazione, le proprie giustificazioni scritte. Ove le suddette giustificazioni non pervengano ovvero Unioncamere non le ritenga condivisibili, si riserva l'insindacabilità di applicare le seguenti penalità:
- fino al … [10%] dell'importo contrattualmente previsto in caso di prima violazione
- fino al … [40%] dell'importo contrattualmente previsto in caso di recidiva
- risoluzione del contratto con effetto immediato, ai sensi degli artt. 1453 e/o 1456 cod. civ. in caso di ulteriori violazioni.

Le penalità sono decurtate direttamente sull'importo del saldo da corrispondere. Rimane impregiudicata la possibilità di agire in sede di rivalsa in caso di eventuali danni subiti da terzi interessati o per le eventuali sanzioni amministrative comminate al Committente.

Le parti di comune accordo adegueranno le clausole di cui al presente articolo e contenute nell'appendice contrattuale al modello di atto giuridico e/o clausole tipo ove predisposte dalla Commissione UE o dall'Autorità Garante italiana ai sensi dell'art. 28, par. 6-8 del GDPR.

Solo l'assunzione delle responsabilità ex art. 28 a livello contrattuale (costituenti quindi specifica obbligazione contrattuale ai sensi dell'art. 1321 del c.c.) potranno consentire – in caso di danno causato da attività del Responsabile - l'attivazione della clausola di salvaguardia di cui all'art. 82, par. 2[8] del GDPR.

Gli stessi soggetti personalizzano e propongono, in allegato al **contratto, convenzione o atto giuridico analogo che definisce gli obblighi reciproci il seguente** documento (che quindi deve essere formalizzato contestualmente, quale

[6] Ad es., lettera di accettazione dell'offerta, etc.
[7] ATTENZIONE: Descrivere la tipologia dei dati personali oggetto di trattamento.
[8] "… Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento…".

elemento integrante e sostanziale del documento contrattuale). Si specifica che il contenuto di seguito riportato deve essere sempre **attentamente valutato e personalizzato** in funzione delle specifiche esigenze e "consistenza" dei trattamenti oggetto di regolamentazione:

ALLEGATO AL CONTRATTO _____

**DISCIPLINA DELLA PROTEZIONE DEI DATI IN QUALITÀ DI RESPONSABILE DEL TRATTAMENTO**
(art. 28 del Regolamento UE 679/2016)

Unioncamere, in qualità di Titolare del trattamento, con riferimento al rapporto contrattuale in oggetto, al fine di adempiere agli obblighi formali e sostanziali proposti dal Regolamento UE 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito anche Regolamento o GDPR), conferma che il contraente opererà quale responsabile esterno del trattamento dei dati ai sensi dell'art. 28 del GDPR per le fasi di sua competenza, così come definite nella scheda tecnica/offerta presentata.

Si specifica, in proposito, che la verifica del possesso dei requisiti di esperienza, capacità ed affidabilità finalizzate a fornire "garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessati" richiesta dall'art. 28, comma 1 del GDPR, è stata effettuata dalla scrivente Unioncamere nell'ambito dell'iter istruttorio presupposto dell'affidamento contrattuale di cui trattasi; in particolare, le misure di sicurezza tecniche, informatiche ed organizzative in atto (**attestate dal legale rappresentante mediante produzione di un documento descrivente il dettaglio delle misure implementate**) sono state valutate come idonee, in relazione alla natura, oggetto, contesto e finalità del trattamento come definito nell'incarico di cui in oggetto.

Con la sottoscrizione del presente atto, che costituisce condizione di efficacia ed esecutività del contratto citato in oggetto, il contraente – nella persona di _____ che agisce in qualità di _____ - accetta la suddetta nomina confermando la diretta ed approfondita conoscenza delle responsabilità che si assume e assicura sotto la propria responsabilità, di aver adempiuto o di adempiere, in funzione delle caratteristiche del trattamento affidato, alle istruzioni di seguito specificate; in proposito, Unioncamere potrà a sua completa discrezione, ove ritenuto necessario, richiedere al contraente una dimostrazione documentale sull'osservanza delle disposizioni impartite ovvero procedere - direttamente o per il tramite di consulenti di propria fiducia - a verifiche ed audit anche presso la sede del contraente.

**Istruzioni impartite**

Il contraente si impegna espressamente:

- a comunicare prontamente al Referente contrattuale/Responsabile dell'esecuzione del contratto del Titolare committente eventuali situazioni sopravvenute (tra cui a puro titolo esemplificativo, sanzioni comminate dal Garante o da Autorità Giudiziarie ordinarie, anche non relative alle attività di trattamento oggetto del presente atto) che, per qualsiasi ragione, possano incidere sulla propria idoneità allo svolgimento dell'incarico;
- a non acquisire dati personali (ove così previsto contrattualmente) ulteriori rispetto a quelli strettamente necessari per l'esecuzione del servizio come definiti nel contratto di cui in oggetto, ed a non utilizzare i dati personali acquisiti per finalità che non siano strettamente attinenti alle attività contrattualmente definite;
- ad autorizzare a compiere operazioni di trattamento di cui al presente atto esclusivamente soggetti che si siano impegnati, per iscritto, all'obbligo di riservatezza e/o al segreto d'ufficio (ques'ultimo se applicabile), impartendo loro adeguate e documentate istruzioni al fine di garantire il rispetto della normativa precedentemente richiamata, delle condizioni di liceità del trattamento e dei vincoli impartiti attraverso il presente atto;
- ove il contratto di cui in oggetto non preveda una autorizzazione generale in proposito, a non ricorrere ad eventuali ulteriori sub-contraenti senza previa autorizzazione scritta di Unioncamere, soprattutto nel caso in cui ciò comporti il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale; l'autorizzazione potrà essere eventualmente rilasciata sulla base di una preventiva verifica di affidabilità di tali soggetti condotta e rendicontata dal Responsabile ad Unioncamere, finalizzata a garantire lo stesso livello di sicurezza nei trattamenti; in caso di autorizzazione, il Responsabile dovrà adottare opportune clausole contrattuali al fine di richiamare in capo ai sub-contraenti l'obbligo di rispettare le misure e gli accorgimenti stabiliti dalla presente designazione nonché un analogo livello di sicurezza adottato dal contraente e valutato come idoneo da Unioncamere *[ATTENZIONE: da personalizzare in funzione dell'autorizzazione generale/specifica che si vuole rilasciare]*

- a seguire le stesse modalità di cui al punto precedente per tutte le eventuali aggiunte o sostituzioni dei sub-contraenti;
- ad adottare procedure di controllo sull'attività svolta dai soggetti autorizzati o sub-responsabili precedentemente identificati, al fine di verificare l'effettivo rispetto da parte di questi ultimi delle misure di sicurezza gestionali e tecniche adottate, degli obblighi di riservatezza e, comunque, delle istruzioni impartite;
- a non comunicare comunque ad ulteriori soggetti terzi (soprattutto se sia possibile qualificare un trasferimento di dati verso paese terzo od organizzazione internazionale) i dati oggetto di trattamento, senza preventiva autorizzazione scritta di Unioncamere;
- ad adottare tutte le misure di sicurezza tecnico-informatiche ed organizzativo-gestionali **dichiarate in fase contrattuale**, da intendersi come adeguate rispetto all'elencazione non tassativa di cui all'art. 32 del GDPR; nell'eventualità di modifica delle stesse (ad es., in caso di modifiche evolutive di infrastrutture, apparati, applicativi di lavoro e modalità gestionali) dovrà essere garantito – ad esito di specifica analisi di impatto – un livello di sicurezza almeno analogo a quello preesistente; in caso contrario, è fatto obbligo di condividere con il Referente contrattuale/Responsabile dell'esecuzione del contratto di Unioncamere le nuove specifiche di trattamento, al fine di consentire la verifica del mantenimento dell'idoneità allo svolgimento dell'incarico;
- a conservare i dati personali oggetto di trattamento per tutto il periodo di tempo necessario per la realizzazione delle attività contrattualmente previste; alla scadenza del contratto ed a seguito del completamento del pagamento delle spettanze (il cui presupposto è la regolare esecuzione del contratto) ovvero all'atto della cessazione per qualsiasi causa dello stesso, il contraente dovrà provvedere a restituire ad Unioncamere i dati personali in qualunque modalità e forma detenuti, provvedendo quindi a cancellarne ogni copia in proprio possesso e confermando l'avvenuta distruzione per iscritto al referente contrattuale del Committente (salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge od altri fini, ad es., contabili, fiscali, ecc.) *[ATTENZIONE: da personalizzare in funzione dell'oggetto e delle caratteristiche della fornitura]*
- a provvedere - nel caso in cui l'attività affidata comporti l'acquisizione diretta di dati personali dagli interessati - al rilascio dell'informativa agli stessi soggetti contenente tutti gli elementi necessari ai sensi dell'art. 13 del Regolamento e ad acquisirne il consenso, ove necessario e con le modalità previste per la specifica attività; il format di documentazione da utilizzare dovrà essere fornito o concordato con Unioncamere;
- ad informare immediatamente Unioncamere in caso di richiesta di esercizio dei diritti di cui agli artt. 15 e ss. del Regolamento pervenuta direttamente al Contraente, ad es., nell'ambito dei contatti anche successivi al primo con gli interessati;
- a fornire ad Unioncamere, a semplice richiesta e secondo le modalità indicate da quest'ultima, i dati e le informazioni necessarie per:
  - ✓ una tempestiva difesa in eventuali procedure instaurate davanti all'Autorità Garante o Giudiziaria per effetto del trattamento dei dati in cui sia coinvolto l'affidatario;
  - ✓ dare tempestivo riscontro all'interessato che eserciti i diritti di cui al punto precedente direttamente nei confronti del Titolare committente.
- a comunicare al Referente contrattuale/Responsabile dell'esecuzione del contratto di Unioncamere, entro il termine tassativo di 36 ore decorrenti dall'avvenuta conoscenza, eventuali violazioni dei dati personali o presunte tali (a puro titolo esemplificativo: accessi abusivi, azione di malware, furto o smarrimento di computer o fascicoli cartacei, incendi o altre calamità...) che abbiano coinvolto i dati oggetto di trattamento, specificando le azioni correttive poste in atto e gli esiti delle stesse, al fine di consentire al Titolare committente l'adempimento degli obblighi di notificazione al Garante e di comunicazione agli interessati, come previsto dagli artt. 33 e 34 del Regolamento;
- in fase di rendicontazione periodica o finale delle attività svolte (sulla base di quanto previsto contrattualmente), a relazionare ad Unioncamere sul buon esito delle attività di trattamento secondo gli standard precedentemente definiti.

La presente designazione è valida per tutto il periodo di durata degli accordi contrattuali e dei successivi eventuali rinnovi o affidamenti aventi lo stesso oggetto, salva richiesta di revisione di una delle parti che dovrà essere formalmente accettata da entrambe. È da ritenere revocata, con effetto immediato e senza obbligo di preavviso, in caso di recesso unilaterale o consensuale dall'incarico citato in premessa.

Nel pregare di restituire alla scrivente Unioncamere una copia del presente allegato datato e firmato per

accettazione, si inviano cordiali saluti.

## CHIARIMENTI IN CASO DI ATI/RTI

In caso di affidamenti ad Associazioni o Raggruppamenti Temporanei di Imprese, in relazione alle specifiche responsabilità derivanti dalla forma di associazione adottata (di tipo orizzontale, verticale o mista), le istruzioni di cui al paragrafo precedente vanno formalizzate:

- all'ATI/RTI, se il trattamento è effettuato unitariamente;
- per ciascuna Società, se il trattamento è effettuato settorialmente, per quanto di rispettiva competenza.

In proposito, si specifica che con la presentazione dell'offerta congiunta,

a) le imprese riunite in RTI/ATI orizzontale assumono una **responsabilità solidale** nei confronti della stazione appaltante;
b) per le imprese riunite in RTI/ATI verticale la responsabilità è invece **limitata all'esecuzione delle prestazioni di rispettiva competenza** (lavori scorporabili o, nel caso di servizi e forniture, prestazioni secondarie), ferma restando la responsabilità della mandataria per l'intero appalto.

## ACQUISIZIONE DI SISTEMI E SERVIZI CON FUNZIONI DI AMMINISTRAZIONE DEI SISTEMI

Gli affidamenti che comportino l'acquisizione di sistemi o servizi di tipo applicativo o infrastrutturale, prevedono di regola attività di **assistenza e manutenzione** svolta direttamente dal soggetto affidatario (o suoi delegati). Tale attività, seppur non ha come obbiettivo o ad oggetto un "trattamento" di dati personali[9] può comportare comunque anche solo "solo incidentalmente" la conoscibilità dei dati, ai soli fini dell'espletamento delle loro consuete attività; tali soggetti sono comunque concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Il punto 3-bis del Provvedimento a carattere generale 27 novembre 2008 del Garante per la protezione dei dati personali "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (in G.U. n. 300 del 24 dicembre 2008) e s.m.i. prevede che nel caso di servizi di amministrazione di sistema affidati in outsourcing, ciò avvenga **nell'ambito della designazione a Responsabile esterno del trattamento** (che in questi casi è quindi necessariamente effettuata).

In questi casi:

a) la valutazione preliminare all'affidamento deve essere "rafforzata" in considerazione della rilevanza e delicatezza di tali peculiari mansioni rispetto ai trattamenti di dati personali svolti per le proprie funzioni istituzionali;
b) l'allegato contrattuale deve contenere anche le seguenti specifiche gestionali:

**Istruzioni impartite**

**…**

Il contraente si impegna espressamente:

- relativamente a quanto prescritto dal Provvedimento del Garante del 27 novembre 2008 e s.m.i., a:
  - ✓ procedere alla designazione individuale degli amministratori di sistema o figura equivalente coinvolti nelle attività di cui in oggetto, previa valutazione delle caratteristiche di esperienza, capacità, e affidabilità, anche in considerazione delle responsabilità che possono derivare in caso di incauta o inidonea designazione;
  - ✓ a riportare, per ciascuna figura coinvolta, l'elencazione degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
  - ✓ a conservare e fornire ad Unioncamere, a semplice richiesta e secondo le modalità indicate da quest'ultima, l'elenco degli amministratori di sistema o figure equivalenti designate;
  - ✓ a verificare periodicamente – anche attraverso idonei sistemi di registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici, che dovranno essere conservati per almeno sei mesi a far data dalla conclusione delle attività contrattuali - l'operato di tali figure in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza adottate; l'esito di tali valutazioni dovrà essere trasmesso ad Unioncamere, a semplice richiesta e secondo le modalità indicate da quest'ultima.

[9] a meno che il database che raccoglie i dati/informazioni non sia residente presso sedi/apparecchiature del contraente ovvero in cloud, nel qual caso è qualificabile almeno il trattamento di "conservazione" dei dati

## ULTERIORI CASISTICHE

### INCARICHI PROFESSIONALI O DI CONSULENZA

Teoricamente, un soggetto esterno – persona fisica - che tratti i dati per conto di un Titolare o Responsabile del trattamento può essere inquadrato nei seguenti schemi:

a) titolare autonomo del trattamento, ad es., quando l'incarico conferito sia connotato da spiccata **autonomia professionale e gestoria**[10]
b) responsabile esterno del trattamento ex 28 del GDPR[11]
c) soggetti autorizzati al trattamento (art. 29 del GDPR e art. 2 quaterdecies, comma 2 del D.Lgs. 196/2003 e s.m.i.[12], anche richiamando una precedente interpretazione del Garante per la Protezione dei dati personali[13] (ove operanti sotto l'autorità diretta del Titolare)

In concreto, la valutazione deve essere effettuata in modo sostanziale, con specifico riguardo allo schema contrattuale alla base del rapporto ed alla concreta regolamentazione delle modalità operative di realizzazione delle attività. Di conseguenza:

- qualora si ricada nelle casistiche di cui alla lett. a, basterà richiamare nel documento contrattuale tale qualifica e l'assunzione diretta da parte del soggetto esterno delle relative responsabilità
- qualora si ricada nella seconda soluzione, si rinvia per il dettaglio delle soluzioni gestionali al precedente capitolo
- nel caso in cui si scelga la soluzione sub c), a tali soggetti dovranno applicarsi idonee clausole contrattuali in riferimento ai trattamenti oggetto dell'incarico stesso, contenenti le eventuali istruzioni specifiche necessarie per l'esecuzione delle attività previste

### CONTRATTI/CONVENZIONI PER LA FORNITURA DI PERSONALE

Nel caso di contratti/convenzioni con soggetti esterni (ad es., Società/Agenzie di somministrazione lavoro) che forniscano personale da impiegare presso le Strutture organizzative di Unioncamere in processi/attività che possano comportare la conoscibilità di dati personali, non si concretizza una "comunicazione" di dati verso una struttura esterna (ovvero di un caso di trattamenti "esternalizzati" nell'ambito della Struttura organizzativa del soggetto esterno); in tali circostanze, l'utilizzo di personale esterno avviene nell'ambito dell'organizzazione del Titolare committente, e non è dunque necessario verificare l'affidabilità della controparte contrattuale e vincolarla ad operare ai sensi dell'art. 28 del GDPR.

In questi casi è però opportuno che i contratti/convenzioni/atti deliberativi rechino la seguente clausola (da personalizzare a cura del RUP/dirigente proponente).

ART. XY TRATTAMENTO DEI DATI PERSONALI

Posto che la realizzazione dell'attività di cui in premessa potrà comportare la conoscibilità – da parte dei soggetti da Voi incaricati - dati personali _____*descrivere*_____ in relazione ai quali Unioncamere è Titolare del trattamento ai sensi dell'art. 4, n. 7 del Regolamento UE 679/2016 (di seguito anche GDPR), si conviene quanto segue.

Nel quadro degli obiettivi generali di tutela della dignità e riservatezza degli interessati promossi dalla normativa richiamata, il contraente garantisce che i professionisti coinvolti siano a conoscenza della normativa rilevante e delle responsabilità relative al corretto trattamento dei dati che essi si assumono nello svolgimento delle attività oggetto della presente convenzione. Per effetto della sottoscrizione della presente convenzione, a tali professionisti è richiesto:

✓ il rispetto dei più elevati standard di segreto professionale, con l'obbligo di mantenere riservati qualsiasi

[10] è il caso ad es., dei componenti del Collegio Sindacale ovvero del revisore legale dei conti (i cui ampi poteri di controllo conferiti dalla normativa di riferimento non sono conciliabili con altre figure previste dalla legge - responsabile, autorizzato - che presuppongono una subordinazione al titolare del trattamento in ordine alla definizione di compiti, istruzioni impartite e vigilanza sull'attività espletata); del notaio, dell'avvocato nell'ambito della procura alle liti, del consulente tecnico di parte, del medico competente in quanto operanti in totale autonomia, responsabilità professionale e con una autonoma organizzazione di mezzi…

[11] "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 (art. 4, par. 1, n. 8)

[12] "I titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta"

[13] Cfr. in particolare https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1507921

notizia, documentazione, dato e informazione concernente direttamente o indirettamente le prestazioni svolte, con esplicito divieto di: utilizzarli per finalità diverse da quelle oggetto della convenzione; divulgarli, comunicarli o renderli disponibili a terzi, in tutto o in parte, senza esplicita autorizzazione scritta di Unioncamere; duplicarli, riprodurli od asportarli dai luoghi di trattamento convenuti;

- ✓ di adottare le procedure, le istruzioni operative e le misure di sicurezza che verranno loro trasferite dal Dirigente responsabile della Struttura organizzativa di allocazione, in qualità di soggetto delegato ad acta dal Titolare del trattamento.

Gli obblighi di riservatezza e segreto professionale rimarranno efficaci - in capo ai singoli professionisti - anche oltre la data di conclusione delle attività di cui alla presente convenzione.

Il rapporto non prevede invece responsabilità relativamente all'ottemperanza ad altri obblighi normativi quali prestazione dell'informativa e acquisizione del consenso dell'interessato che restano, qualora necessari, in capo al Titolare del trattamento.

ALLEGATO 3

UNIONCAMERE

# SGDP - SISTEMA DI GESTIONE DEI DATI PERSONALI
# Linee guida per la realizzazione di una valutazione di impatto del trattamento di dati (DPIA)

ai sensi del Regolamento UE 679/2016

## SOMMARIO

# PREMESSA

## SCOPO E CAMPO DI APPLICAZIONE

Il presente documento di indirizzo ha lo scopo di fornire indicazioni utili in grado di coadiuvare Unioncamere e gli apicali dell'Enti a ciò delegati, nella più veloce e completa definizione di un processo - e relativi strumenti operativi - per la gestione degli adempimenti di cui agli artt. 35 e 36 del GDPR.

Le indicazioni qui definite sono portate a conoscenza, anche attraverso attività di sensibilizzazione o formazione, di tutti i Dirigenti, Quadri, funzionari o, comunque, referenti delle Aree/Uffici di Unioncamere potenzialmente coinvolti nella stessa.

## INTRODUZIONE ALLA DPIA

Una valutazione d'impatto sulla protezione dei dati (di seguito anche DPIA) è un **processo** finalizzato a:

- descrivere il trattamento, valutarne la necessità e la proporzionalità rispetto agli scopi
- valutare l'esistenza (origine, natura, particolarità e gravità) di un rischio per gli interessati
- determinare l'opportunità/necessità di adottare adeguate misure per mitigare il rischio rilevato

La DPIA è lo strumento che consente al Titolare di garantire e dimostrare di operare in conformità al GDPR, ovvero secondo:

a) il principio di **accountability**, rendendo esplicito l'approccio ai processi di trattamenti basatO sul rischio, potendo così documentare le valutazioni e le decisioni assunte a fronte di eventuali controlli
b) i principi della **privacy by design & by default**, consentendo di impostare fin dalla progettazione (e per impostazione predefinita) gli strumenti idonei a dimostrare la liceità del trattamento e le relative misure implementate

La DPIA è un obbligo del Titolare del trattamento; ne consegue che, l'adempimento potrebbe in teoria essere delegato materialmente ad es., ad un Responsabile del trattamento, ma la metodologia utilizzata e gli esiti finali della stessa devono essere condivisi e verificati dal Titolare, che quindi deve farla propria in quanto potrebbe essere chiamato a risponderne.
La DPIA deve essere effettuata:

1. prima di procedere al trattamento[1] (ad es., in fase di ideazione/progettazione di un nuovo processo di trattamento o progetto)
2. per trattamenti già in atto, nel caso di variazione del rischio dovute a modifica delle finalità, delle modalità di realizzazione (ad es., prevedendo l'utilizzo di nuove tecnologie), emergere di nuove vulnerabilità, mutamento del contesto organizzativo del trattamento etc.

Può essere utile, in premessa, individuare dei **check-point**, ovvero delle circostanze o iniziative che dovrebbero indurre il Titolare del trattamento a valutare l'attivazione del processo di DPIA; nel contesto di Unioncamere, tali check-point possono essere individuati, a puro titolo esemplificativo, in:

- nuove progettualità avviate a partire dalla partecipazione a fonti di finanziamento pubblico ovvero sulla base di partnership con altre PPAA od organizzazioni private
- nuovi servizi informatici sviluppati in ambito progettuale, che insistono su trattamenti esistenti o che introducano nuovi trattamenti
- cambiamenti significativi a livello organizzativo, con effetti su processi e sistemi di trattamento

In queste ed altre circostanze, una singola valutazione può:

- esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi (art. 35, par. 1)
- coinvolgere più Titolari (o Contitolari), ad esempio quando autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni o quando diversi titolari del trattamento progettano di introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata (considerando 92)

Il Titolare del trattamento coinvolge il RPD (art. 35, par. 2 e art. 39, par. 1, lett. c del GDPR) durante l'iter di gestione di una DPIA ad es.:

- richiedendo un parere sulla necessità/obbligo di esecuzione della DPIA stessa
- per sorvegliarne lo svolgimento

[1] In proposito, il considerando 89 del GDPR specifica che l'esigenza può riscontrarsi in relazione a "trattamenti di nuovo tipo e in relazione ai quali il titolare del trattamento non abbia ancora effettuato una DPIA, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale"

- richiedendo un parere finale sugli esiti della stessa, anche al fine di valutare se procedere o meno alla consultazione dell'Autorità

Gli esiti della DPIA dovrebbero essere inseriti nel Registro dei trattamenti (come "nuovo" trattamento ovvero in modifica delle caratteristiche di un trattamento già censito).

## RIFERIMENTI NORMATIVI

La presente procedura risponde ai seguenti requisiti normativi:

1. Valutazione d'impatto sulla protezione dei dati (art. 35 GDPR)
2. Consultazione preventiva (art. 36 GDPR)
3. WP29 "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" (wp248 rev.01 del 04/10/2017)
4. Garante per la Protezione dei dati Personali, Provvedimento n. 467 dell'11/10/2018 "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679", in GU n. 269 del 19/11/2018
5. WP250rev.01 "Guidelines on Personal data breach notification under Regulation 2016/679", adottate il 03/10/2017 e riemesse il 06/02/2018
6. WP29 "Linee guida sui responsabili della protezione dei dati" (wp243 rev. 01 del 05/04/2017)
7. DIG - Dipartimento di Ingegneria Gestionale del Politecnico di Milano, Osservatorio Information Security & Privacy, "Linee guida per la Data Protection Impact Assessment", rev. 2018
8. ENISA - European Union Agency for Network and Information Security, "Handbook on Security of Personal Data Processing", rev. dicembre 2017
9. ISO/IEC 31010:2009 "Risk management – Risk assessment techniques", ed in particolare la tecnica "Consequence/probability matrix" di cui alla sezione B.29 (pag. 82)
10. …

## ACRONIMI E DEFINIZIONI UTILIZZATE

| | |
|---|---|
| GDPR | Regolamento UE 2016/679 (General Data Protection Regulation) |
| Codice | D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. 101/2018 |
| Garante | Garante per la protezione dei dati personali |
| RPD | Responsabile della protezione dei dati |
| Delegato del Titolare | Soggetto che, secondo le deleghe/procure formalizzate ed il sistema di gestione della privacy, garantisce specifiche funzioni ai fini della *compliance* al GDPR |
| SG | Segretario Generale di Unioncamere |
| DPIA | Data Protection Impact Analysis (Valutazione d'Impatto sulla Protezione dei Dati) |
| 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 |

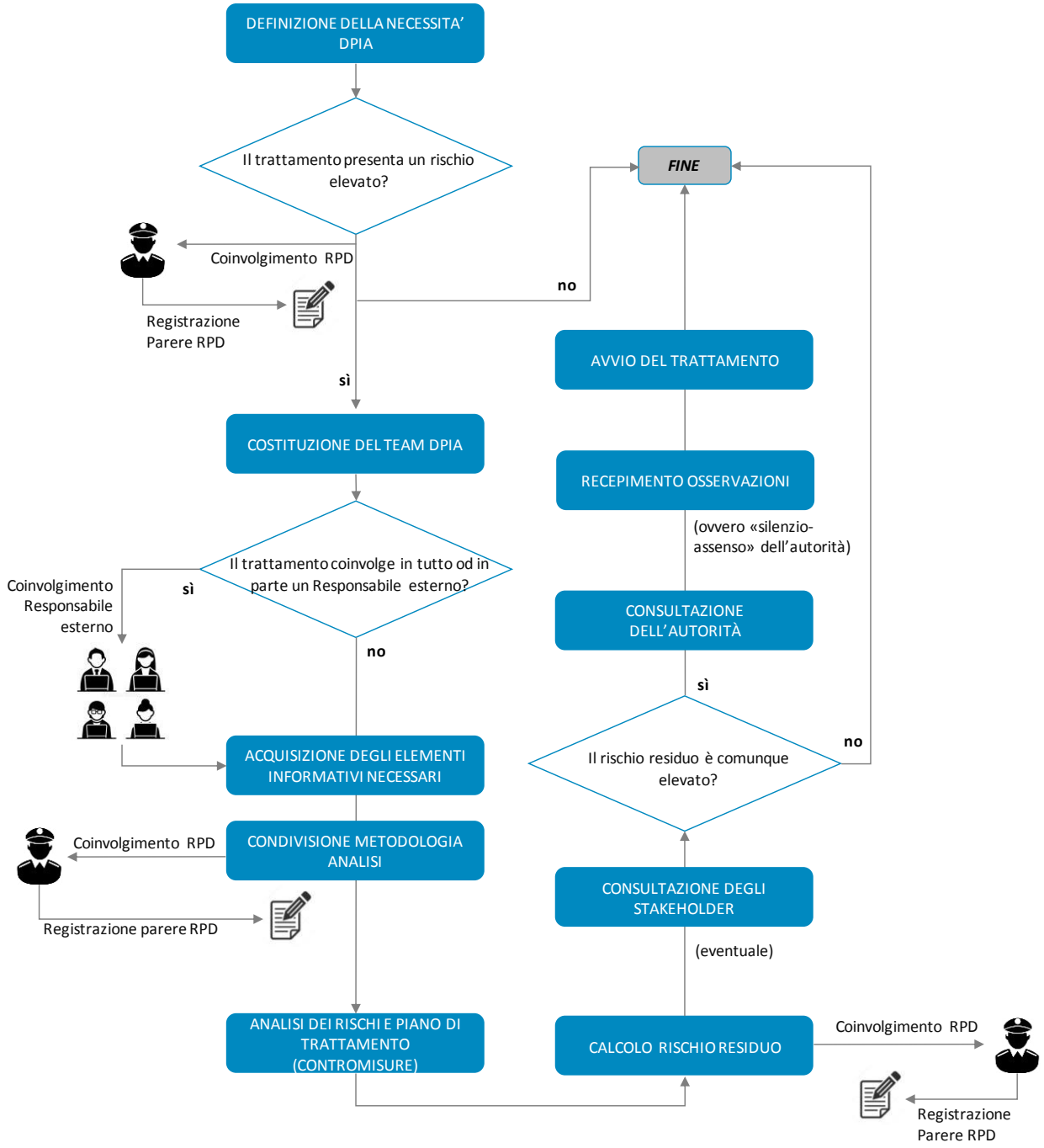
| | |
|---|---|
| Profilazione | qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica |
| Larga scala | Una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale che potrebbero incidere su un vasto numero di interessati |
| Rischio | Uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità |
| | |

## MATRICE DELLA REDAZIONE E DELLE REVISIONI

| Data | Stato | Descrizione | Approvazione |
|---|---|---|---|
| 13/12x/2018 | Approvato | Rev 0 – I$^{a}$ emissione | Delibera del Comitato esecutivo del 13/12/2018 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## FASI DEL PROCESSO

La gestione di una DPIA può riassumersi nelle fasi di seguito rappresentate.




### DEFINIZIONE DELLA NECESSITÀ DI REALIZZAZIONE DELLA DPIA

A norma dell'art. 35 del GDPR, la DPIA è necessaria quando il trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"; tale situazione è riscontrabile in particolare ove il trattamento consista in:

- ✓ 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** o incidono in modo analogo significativamente su dette persone fisiche;
- ✓ il **trattamento, su larga scala**, di categorie **particolari** di dati personali (art. 9 GDPR) o di dati relativi a **condanne penali e a reati** (art. 10)
- ✓ a **sorveglianza sistematica su larga scala** di una zona accessibile al pubblico, in particolare se effettuata mediante dispositivi optoelettronici

A maggior puntualizzazione delle previsioni normative, il Garante italiano ha definito un elenco non esaustivo di trattamenti che obbligano un Titolare alla realizzazione della DPIA. Tale posizione deriva da una autonoma scelta, di valutare le seguenti singole tipologie di trattamento come altamente rischiose per i diritti e le libertà degli interessati:

1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "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"
2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi)
3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) da i quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)
7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01
8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment)
10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento

L'elenco di cui sopra può essere modificato, quindi il soggetto che effettua la valutazione dovrà sempre preliminarmente verificarne l'attendibilità ed aggiornamento sul sito istituzionale dell'Autorità Garante.

In quanto elenco non esaustivo, rimane ferma – in tutti i casi in cui il trattamento non ricada in una delle ipotesi di cui sopra – la necessità di seguire le indicazioni del WP 29, che identifica 9 criteri, definendo la DPIA come obbligatoria (riscontrando un livello di "rischio inerente" potenzialmente elevato) nel caso in cui il trattamento in analisi soddisfi **almeno due di essi**:

1. valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione[2]
2. processo decisionale automatizzato che ha effetti giuridici o incida in modo analogo significativamente sui diritti degli interessati
3. monitoraggio sistematico, utilizzato per osservare, monitorare o controllare gli interessati[3]
4. impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto[4]
5. creazione di corrispondenze o combinazione/raffronto di insiemi di dati[5]
6. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative[6]
7. dati sensibili o dati aventi carattere altamente personale[7]
8. trattamento di dati su larga scala (a livello regionale, nazionale o sovranazionale)[8]
9. dati relativi a interessati vulnerabili[9]

Una analoga valutazione dovrebbe essere realizzata in tutti i casi in cui **si modifichino le caratteristiche del trattamento o dei mezzi utilizzati** per realizzarlo.

Per identificare se – per effetto del trattamento ipotizzato – si ricada in una o più dei 9 criteri elencati, potrà essere di aiuto la compilazione di tutti o parte dei campi riportati nell'Allegato 2 al presente documento (sezioni A e B).

La DPIA **non è necessaria**, comunque:
a) quando il trattamento rientri in una delle casistiche di esclusione che saranno espressamente definite dall'Autorità Garante nazionale e dal Comitato dei Garanti europei
b) quando il trattamento non è tale da presentare un "rischio elevato" (ovvero quando, secondo le indicazioni del WP29 non si ricada in almeno due delle casistiche precedentemente elencate,)
c) per trattamenti dei tutto simili ad altri per i quali sia già stata effettuata una DPIA
d) quando il trattamento sia obbligatorio per legge (nazionale o comunitaria), nel caso in cui quindi la base giuridica sia rinvenibile in un obbligo legale (art. 6, par. 1, lett. c) o in un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare (art. 6, par. 1, lett. e), sempre che:
   - ✓ la normativa disciplini il trattamento specifico o l'insieme di trattamenti in questione e
   - ✓ sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica[10]

E' da specificare comunque che, anche ove si ricada nell'ipotesi sub b) secondo un **approccio cautelativo** le specifiche circostanze del caso dovrebbero comunque poter indurre il Titolare del trattamento (o suo delegato) a predisporre una DPIA quale buona prassi e strumento di accountability.

---

[2] 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*")

[3] ivi inclusi, ad es., i dati raccolti tramite reti (es., internet) o *"la sorveglianza sistematica su larga scala di una zona accessibile al pubblico*"; il concetto di "sistematico" va inteso secondo uno o più dei seguenti criteri: - effettuato secondo un sistema; pre-organizzato, organizzato o metodico; effettuato nell'ambito di un piano generale per la raccolta dei dati; - svolto come parte di una strategia

[4] trattamenti che mirano a consentire, modificare o rifiutare l'esercizio di un diritto degli interessati ovvero l'accesso degli interessati a un servizio oppure la stipula di un contratto (ad es., screening dei clienti di una banca attraverso i dati della Centrale Rischi al fine di stabilire se ammetterli o meno al finanziamento)

[5] ad esempio, nel caso di interconnessione di banche dati: 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

[6] Ad es., combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, Internet of Things, etc.

[7] categorie particolari di dati personali così come definite all'articolo 9, dati personali relativi a condanne penali o reati di cui all'articolo 10; dati personali che consentono la geo-localizzazione (ubicazione); dati relativi alle comunicazioni elettroniche (ad es., indirizzo IP, email, agende digitali…); dati finanziari (situazione economica o patrimoniale, rischio solvibilità, etc.)

[8] In proposito, le linee guida WP 29 consigliano i seguenti criteri per determinare se il trattamento sia svolto su larga scala: - numero di soggetti interessati, sia come numero specifico che come percentuale rispetto all'universo di interessati di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati; - durata o persistenza dell'attività di trattamento; - estensione geografica del trattamento

[9] Ovvero tutte quelle categorie di persone che potrebbero essere coartate nelle proprie volontà a causa dello squilibrio di potere tra gli stessi e il titolare del trattamento (es., minori, dipendenti, infermi di mente, richiedenti asilo o anziani, pazienti…)

[10] ad es., nell'ambito delle AIR (Analisi di Impatto della Regolazione), ATN (Analisi Tecnico Normativa) e VIR (Verifica di Impatto della Regolamentazione)

Qualora non si ricada in una di queste precondizioni di esclusione, il Process Owner ovvero:

a) il soggetto "delegato del Titolare"[11] competente *ratione materiae,* nel cui ambito di responsabilità ricade il trattamento oggetto di analisi
b) per trattamenti trasversali all'Organizzazione o specifici progetti, il responsabile individuato dal Comitato Esecutivo o dal SG (delegato *ad acta*)

provvede alla valutazione preliminare sulla necessità di eseguire la DPIA sulla base degli elementi conoscitivi a propria disposizione; in questa fase può essere richiesto un parere al RPD sugli esiti della stessa.

In Allegato 1 è riportato un modello di **Valutazione d'impatto semplificato** e del relativo algoritmo di calcolo utilizzabile a tali fini. La tabella posiziona in verticale - in una scala da 1 a 5, in cui 1 è il livello minimo di rischio (trascurabile) – quattro criteri di valutazione e relativi parametri, connessi alla "consistenza" del trattamento, alla "qualità" dei dati, alla "tipologia di interessati" coinvolti ed alla "tipologia/finalità del trattamento" stesso. Il delegato provvederà a valorizzare ciascuno dei 4 criteri a seconda dei parametri caratterizzanti il trattamento in analisi (il punteggio più elevato contiene il punteggio minore). In proposito, si specifica che, in coerenza con le indicazioni del WP 29:

↘ le 9 casistiche di cui sopra sono state posizionate tutte tra i livelli 4 e 5 (in quanto potenzialmente determinanti un rischio elevato per gli interessati)
↘ l'algoritmo di calcolo prevede la media dei valori assegnati ai 4 criteri, tranne nel caso in cui si valorizzino almeno due parametri al livello 4, il che determina comunque un impatto complessivo identificato almeno come "significativo"

Le informazioni disponibili e le conclusioni della valutazione preliminare devono essere adeguatamente **verbalizzate**, compreso il **parere del RPD richiesto e formalizzato**. Il Process Owner deve, in particolare, giustificare e documentare tutti i casi in cui, pur presentando un trattamento due o più criteri sopra evidenziati, sia giudicato tale da non "presentare un rischio elevato" e quindi da non richiedere la DPIA.

Nel caso in cui si verificassero conflitti decisionali in questa fase, ad es. in relazione alla decisione di NON procedere con la DPIA, il verbale finale deve essere rimesso alla valutazione del SG.

## COSTITUZIONE DEL TEAM DPIA

Ove la fase precedente dia esito positivo, ovvero sia necessario effettuare una specifica DPIA ai sensi dell'art. 35 del GDPR, il Process Owner di cui al par. precedente provvede ad attivare il Team DPIA composto almeno da:

- lo stesso Process Owner, che lo coordina
- uno o più referenti della Struttura operativa del Process Owner e/o di ulteriori strutture interne (Aree/Uffici di UC) od esterne (ad es., CCIAA nel caso di progetti "nazionali") eventualmente coinvolte nel trattamento oggetto di analisi
- un referente dell'Area Legale ed Amministrativa;
- un referente CED ove il trattamento debba essere gestito da sistemi informativi/banche dati gestite internamente ad UC
- il RPD (ove nominato) e/o uno o più specialisti del/delle società esterne/in house eventualmente coinvolte nel trattamento[12]
- l'eventuale consulenza tecnica o giuridica qualora necessaria.

In proposito è importante sottolineare come condurre una DPIA significa **lavorare in Team** all'interno dell'Organizzazione: una valutazione è tanto più efficace quando coinvolge e consulta soggetti provenienti da diversi settori dell'Organizzazione e/o esterni, in grado ciascuno di individuare differenti rischi - da diversi punti di vista - e soluzioni basate sulla propria esperienza.

Il Processo owner provvede ad assegnare al Team e/o a singoli referenti le responsabilità connesse alle fasi successive.

## ACQUISIZIONE DEGLI ELEMENTI INFORMATIVI NECESSARI

Il Team così costituito supporta il Process Owner nella rilevazione ed analisi di tutte le informazioni di cui all'All. 2, necessarie per:

a) identificare "la natura, l'oggetto, il contesto e le finalità del trattamento", come richiesto dall'art. 35

[11] cfr. in proposito SGDP_ Modello organizzativo, ruoli e sistema di responsabilità

[12] A norma dell'art. 28, par. 3, lett. e) ed f) del GDPR, il Responsabile del trattamento "*assiste il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione...*"; cfr. in proposito il documento SGDP_ Linee guida per l'allocazione delle responsabilità a soggetti esterni

b) essere in grado di valutare la necessità, liceità e proporzionalità del trattamento
c) lo sviluppo successivo della vera e propria analisi dei rischi

Gli elementi informativi minimi, in proposito, sono i seguenti:
- la natura, l'ambito, il contesto del trattamento
- le finalità del trattamento (determinate, esplicite e legittime)
- la base giuridica del trattamento (tra quelle di cui all'art. 6)
- la tipologia di dati (che devono essere adeguati, pertinenti e limitati a quanto necessario)
- la tipologia di interessati coinvolti
- i tempi di conservazione (limitati allo stretto indispensabile)
- l'individuazione delle risorse/asset utilizzate per il trattamento (hw, sw, reti, persone, etc.)

Alcuni elementi di maggiore approfondimento possono inoltre essere utili per verificare – in sede di prima analisi - le misure di tipo organizzativo e tecnico adottate a prescindere dal livello di rischio del trattamento, vale a dire:
- l'assegnazione delle responsabilità per il trattamento (interne ed esterne al titolare)
- le garanzie adottate per la minimizzazione, l'esattezza e l'aggiornamento dei dati
- le modalità di rilascio dell'informativa ed (eventuale) acquisizione del consenso
- i canali disponibili e le garanzie in merito all'esercizio dei diritti
- le garanzie adottate in caso di trasferimento dei dati in paesi od organizzazioni terze

Infatti, il GDPR introduce un principio di proporzionalità delle misure da ritenere adeguate per garantire la conformità del trattamento al GDPR; la valutazione di adeguatezza però parte da una preliminare analisi dei principi base del GDPR (artt. 5 e 6) e prevede l'adozione di soluzioni incrementali in base a condizioni di rischio oggetto di successiva valutazione.

In proposito, quindi, il Team deve verificare che vi siano tutti i presupposti per effettuare un **trattamento conforme ai requisiti di legittimità previsti dal GDPR**. Qualora tutte le verifiche portino ad un esisto positivo, si può procedere ad effettuare la valutazione successiva; qualora invece le verifiche portino ad un esito negativo il trattamento non può essere effettuato, almeno con le finalità, modalità e mezzi previsti all'interno dell'analisi appena effettuata.

In ogni caso, la formalizzazione degli esiti della rilevazione (che costituiscono dato di input per le decisioni conseguenti in merito alla legittimità del trattamento) ricade nella responsabilità del Process Owner.

## VALUTAZIONE DEI RISCHI

Questa fase è idealmente scomponibile in tre sotto-fasi:
1. **analisi approfondita sui trattamenti e delle diverse categorie di rischio cui i dati personali sono soggetti nell'ambito dei trattamenti**
2. stima in termini di **probabilità delle cause e di gravità degli effetti** di una eventuale violazione dei dati (rischio inerente)
3. **identificazione delle contromisure** (di natura infrastrutturale, applicativa o organizzativo-gestionale)
4. **formalizzazione delle risultanze** finali e **condivisione** con gli stakeholder

La valutazione del rischio e l'individuazione delle misure di sicurezza ai fini della DPIA si intersecano, anche dal punto di vista temporale, con l'individuazione delle misure tecniche ed organizzative adeguate di cui all'art. 25 par. 1 del GDPR che, com'è noto, devono essere definite "al momento di determinare i mezzi del trattamento"; tale momento può essere fatto coincidere con la locuzione "prima di procedere al trattamento" di cui all'art. 35 del GDPR. Entrambi gli adempimenti convergono, quindi, in fase di progettazione del trattamento (privacy by design), di cui la DPIA costituisce dato di input.

La metodologia utilizzata per questa fase (ove diversa da quella esplicitata nelle presenti linee guida) dovrà essere **condivisa con il RPD**[13].

### ANALISI DEI TRATTAMENTI ED IDENTIFICAZIONE DELLE CATEGORIE DI RISCHIO

L'analisi approfondita dei trattamenti può essere supportata da fonti informative già disponibili all'interno di UC per descrivere il progetto (ad es., progetti/convenzioni in fase di studio, diagramma dei flussi informativi tra i vari soggetti,

[13] Cfr. indicazioni previste dal WP29

sistemi o processi; sequenza prevista delle operazioni di gestione dei dati ed interazione con gli interessati, rapporti sull'uso delle informazioni, mappe informative, registri di asset informativi...) ovvero a partire da quanto già raccolto nel par. "ACQUISIZIONE DEGLI ELEMENTI INFORMATIVI NECESSARI" ai fini della verifica di legittimità del trattamento stesso.

Una volta definita la legittimità del trattamento, è necessario concentrarsi sulla identificazione:

- delle possibili **minacce**, ovvero dei possibili eventi che possono esporre il trattamento ed i dati (e quindi i relativi interessati) a rischi di protezione e/o di sicurezza (informatica o fisica), e le possibili modalità realizzative delle stesse
- delle **vulnerabilità**, ovvero delle possibili criticità gestionali o tecniche di cui si può ipotizzare l'esistenza
- di conseguenza, uno **scenario di rischio** il più possibile attinente al trattamento in questione

Di seguito si propone una tabella che, a partire dall'art. 32, par. 2 del GDPR e dalle Linee guida WP29 in materia di data breach, dovrebbe guidare l'identificazione degli elementi su-esposti:

| Tipologia di violazione | Descrizione (minacce) |
|---|---|
| **Distruzione** | Indisponibilità irreversibile o di lunga durata di dati personali trattati dal Titolare. La violazione può essere relativa a:<br>• eliminazione logica non autorizzata (es. cancellazione dei dati)<br>• eliminazione fisica (es. danneggiamento o distruzione dei supporti di memorizzazione o dei documenti cartacei)<br>• eliminazione logica o fisica dei dati in formato elettronico, il cui ripristino da documenti cartacei è possibile ma con un impiego di tempo elevato, tale da poter generare effetti sull'Interessato.<br>In questo scenario, i dati personali possono essere recuperati solo:<br>✓ direttamente dall'Interessato<br>✓ da fonti esterne quali fonti pubbliche e/o di terze parti (es: Pubbliche Amministrazioni);<br>✓ da archivi cartacei (in caso di distruzione, il recupero da tali archivi si suppone estremamente complesso, di lunga durata e con il rischio di ottenere dati non aggiornati) |
| **Indisponibilità** | Indisponibilità, irreversibile o temporanea, dei mezzi e degli strumenti necessari per effettuare il trattamento dei dati da parte degli interessati o del Titolare per l'erogazione di servizi richiesti o per conto dell'Interessato. L'Indisponibilità non implica la distruzione dei dati personali. L'Indisponibilità irreversibile di un mezzo o strumento richiede l'adozione di nuovi mezzi o strumenti per accedere ai dati. Tale violazione può essere relativa a:<br>• indisponibilità dei sistemi e dei servizi informatici mediante i quali le informazioni sono accessibili (es: in caso di attacco informatico)<br>• indisponibilità di mezzi e strumenti necessari per l'accesso alle informazioni (es: perdita di una chiave di decifratura o di un token hardware di accesso con la possibilità di accedere ai dati in backup o altri archivi)<br>• indisponibilità degli strumenti atti a identificare l'informazione all'interno di grandi archivi cartacei o elettronici<br>• degrado prestazionale dei servizi informatici, che determina l'impossibilità di perfezionare operazioni di trattamento<br>• modifiche tecnologiche che rendono impossibile la decodifica di dati rappresentati secondo particolari formati di memorizzazione. |
| **Perdita** | Perdita del supporto fisico di memorizzazione dei dati (es. privazione, sottrazione, smarrimento dei dispositivi contenti i dati oppure dei documenti cartacei).<br>La Perdita di un supporto fisico di memorizzazione dei dati non implica che si sia verificata anche un'altra violazione quale Distruzione, Indisponibilità, Accesso o Divulgazione: ad esempio, un disco DVD perso può contenere una copia cifrata[14] di dati. |
| **Alterazione** | Alterazione non autorizzata dei dati, che può determinare:<br>• la comunicazione di informazioni erronee a enti esterni (es. istituzioni, società, persone, ecc..) o al pubblico (Internet);<br>• errori nel trattamento o trattamento non conforme<br>• decisioni errate con effetti sull'Interessato.<br>In alcuni casi l'Alterazione può seguire un Accesso ai dati da parte di soggetti non aventi diritto. In altri casi può essere dovuta ad errori nel trattamento. |
| **Divulgazione** | Comunicazione o diffusione non autorizzate od improprie dei dati personali, non corrispondenti a informazioni di pubblico dominio, verso terze parti, anche se non note o identificabili.<br>In alcuni casi la Divulgazione può seguire un Accesso ai dati da parte di soggetti non aventi diritto. In altri casi può essere dovuta a trattamenti non conformi di dati riservati. |

[14] La cifratura dei dati, per essere efficace, richiede che le chiavi di cifratura siano integre, non violate e non divulgate

| | |
|---|---|
| **Accesso** | Effettivo accesso (anche in sola visualizzazione) ai dati trattati da parte di soggetti non aventi diritto al momento della violazione. L'Accesso ai dati non implica che si sia verificata anche un'altra violazione quale Distruzione, Alterazione o Divulgazione: il soggetto non avente diritto potrebbe utilizzare a proprio favore le informazioni ricavabili dai dati senza distruggerli, alterarli o divulgarli. |

*(fonte: DIG Politecnico di Milano, Linee Guida per la Data Protection Impact Assessment)*

Ognuna delle minacce sopra esposte può dar luogo ad uno scenario di rischio che coinvolge una o più proprietà dei dati personali; in proposito è ipotizzabile – seguendo un principio di prevalenza – la seguente tabella di correlazione:

| | **Tipologia di violazione** | | | | | |
|---|---|---|---|---|---|---|
| **Proprietà dei dati** | Distruzione | Indisponibilità | Perdita | Alterazione | Divulgazione | Accesso |
| Disponibilità | ☑ | ☑ | ☑ | | | |
| Integrità | | | | ☑ | | |
| Riservatezza | | | | | ☑ | ☑ |

Connesse con le tipologie di violazione, le minacce identificate precedentemente costituiscono pertanto la causa (sia essa accidentale o illecita) della compromissione delle proprietà di Riservatezza, Integrità e Disponibilità dei dati, ove tale compromissione sia in grado di causare un danno (fisico, materiale, morale) agli interessati.

## VALUTAZIONE DEL RISCHIO

### Stima della gravità del rischio

A partire dagli elementi rilevati in sede di pre-analisi (necessità di realizzazione delle DPIA), la metodologia proposta prevede di valutare, per ciascuna delle "proprietà" dei dati (RID) che potrebbe essere compromessa da una violazione, l'impatto sui diritti e sulle libertà fondamentali delle persone fisiche, secondo quanto suggerito nella seguente tabella:

| **Livello d'impatto** | **Descrizione** | **Possibili esempi** |
|---|---|---|
| **Basso** | Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema | Tempo trascorso reinserendo informazioni, fastidi, irritazioni, etc. |
| **Medio** | Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà | Costi aggiuntivi, rifiuto/impossibilità di accesso ai servizi, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc. |
| **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. |
| **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. |

*(fonte: ENISA, Handbook on Security of Personal Data Processing)*

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. Come tutte le valutazioni qualitative, il livello attribuito dovrebbe essere oggettivato attraverso la documentazione delle "assunzioni" intese quali argomentazioni utilizzate per giungere a quel risultato.

| | Livello di gravità | | | |
|---|---|---|---|---|
| **Proprietà dei dati** | Basso | Medio | Alto | Molto Alto |
| Disponibilità | ☑ | | | |
| Integrità | ☑ | | | |
| Riservatezza | | | | ☑ |

*(esempio di applicazione della metodologia)*

**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 da considerare come il risultato finale della valutazione del parametro "gravità", relativo al trattamento complessivo dei dati personali in analisi.**
Naturalmente, l'aver circoscritto minacce e requisito dei dati di maggior impatto per la protezione degli interessati agevolerà l'identificazione successiva del parametro di probabilità di accadimento e l'individuazione della tipologia e livello di implementazione delle misure di sicurezza.

## Stima della probabilità del rischio

Considerando lo scenario di rischio precedentemente individuato, è possibile procedere alla individuazione della **probabilità** di accadimento di una violazione di dati personali. Nella seguente tabella si propone quindi una metodologia di valorizzazione basata su quattro diverse aree di valutazione che interessano gli ambienti di elaborazione e trattamento dei dati (che sono direttamente rilevanti per la concretizzazione delle minacce), 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 seguente riassume un set di valutazioni da effettuare ai fini della valutazione della probabilità di occorrenza di una minaccia.

| ↘ **Risorse di rete e tecniche (hardware e software)** | |
|---|---|
| **Qualche parte del trattamento dei dati personali sarà 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. |
| **Sarà 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. |
| **Il sistema di trattamento dei dati personali sarà 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 sono autorizzate a tale accesso). |
| **Le persone non autorizzate potranno 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). |
| **Il sistema di trattamento dei dati personali sarà 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. |
| ↘ **Processi / procedure relativi all'operazione di trattamento dei dati** | |

| | |
|---|---|
| **I ruoli e le responsabilità relativi al trattamento dei dati personali saranno 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. |
| **L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione sarà 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. |
| **I dipendenti saranno 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. |
| **I dipendenti saranno 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. |
| **Le attività di elaborazione dei dati personali potranno essere eseguite senza la creazione di file di registro?** | La mancanza di adeguati meccanismi di registrazione e monitoraggio può aumentare l'abuso intenzionale o accidentale di processi/ procedure e risorse, con conseguente abuso di dati personali. |
| **↘ Diverse parti e persone coinvolte nell'operazione di trattamento** | |
| **Il trattamento dei dati personali sarà 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. |
| **Qualche parte dell'operazione di trattamento dei dati sarà 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. |
| **Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali saranno 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. |
| **Il personale coinvolto nel trattamento di dati personali 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. |
| **Le persone / le parti coinvolte nell'operazione di trattamento dei dati dovranno 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. |
| **↘ Settore di operatività e scala del trattamento** | |
| **Si ritiene che il settore di operatività in cui si inserisce il trattamento 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. |
| **L'Organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?** | Se l'organizzazione è già stata attaccata o ci sono indicazioni che questo potrebbe essere stato il caso, è necessario prendere ulteriori misure per prevenire eventi simili in futuro. |
| **Hai ricevuto in passato notifiche e / o reclami riguardo alla sicurezza del sistema informatico nell'ultimo anno?** | Bug di sicurezza / vulnerabilità presenti possono essere sfruttati per eseguire attacchi (cyber o fisici) ad altri 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. |

| | |
|---|---|
| **L'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). |
| **Esistono best practice di sicurezza specifiche per il tuo settore di operatività da considerare adeguatamente?** | 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. |

*(fonte: ENISA, Handbook on Security of Personal Data Processing)*

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.

| **Area di valutazione** | **Probabilità** | |
|---|---|---|
| | **livello** | **punteggio** |
| Risorse di rete e tecniche (hardware e software) | Basso | 1 |
| | Medio | 2 |
| | Alto | 3 |
| Processi / procedure relativi all'operazione di trattamento dei dati | Basso | 1 |
| | Medio | 2 |
| | Alto | 3 |
| Diverse parti e persone coinvolte nell'operazione di trattamento | Basso | 1 |
| | Medio | 2 |
| | Alto | 3 |
| Settore di operatività e scala del trattamento | Basso | 1 |
| | Medio | 2 |
| | Alto | 3 |

*(fonte: ENISA, Handbook on Security of Personal Data Processing)*

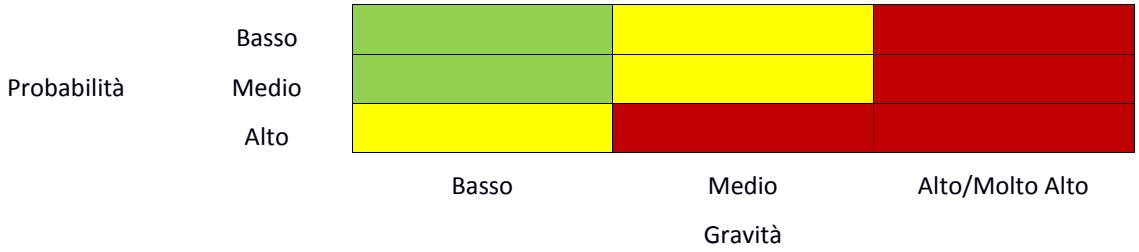
| **Livello probabilità** | **Somma dei punteggi attribuiti alle quattro aree di valutazione** |
|---|---|
| **Basso** | 4 - 5 |
| **Medio** | 6 - 8 |
| **Alto** | 9 -12 |

*(fonte: ENISA, Handbook on Security of Personal Data Processing)*

Il valore della probabilità di occorrenza di una violazione di dati viene calcolato dopo aver sommato i quattro diversi punteggi ottenuti e confrontato il risultato complessivo alle somme riportate nella tabella finale.

## Valutazione del rischio inerente

Dopo aver valorizzato i due parametri (gravità e probabilità di accadimento), la valutazione finale del rischio è desumibile dal posizionamento dei valori nella seguente tabella




*(fonte: ENISA, Handbook on Security of Personal Data Processing)*

I livelli di rischio sono stati allocati sulle celle in funzione del peso assegnato dal modello alle due variabili (probabilità e conseguenze). E' giustificabile, nel contesto del modello in argomento, **assegnare un maggior peso alla variabile "gravità"** (ovvero quella che determina il grado di danno causabile agli interessati in caso di violazione dei dati) rispetto alla variabile probabilistica, in **quanto l'obiettivo della valutazione è proprio incentrato sulla protezione degli interessati**. Tale operazione di "ri-configurazione" della matrice è consentita dalla metodologia utilizzata[15].

L'operazione finale è la comparazione del livello di rischio inerente rilevato con la soglia di "rischio accettabile"; ove i due valori non fossero compatibili, si procederà con la selezione delle contromisure da implementare.

## IDENTIFICAZIONE DELLE CONTROMISURE

### Piano di trattamento del rischio

Obiettivo di questa fase è identificare le misure necessarie a garantire un'adeguata mitigazione di probabilità e/o impatti rilevati precedentemente.
Al fine di agire sugli impatti (gravità del danno derivante da una violazione) potrebbe essere necessario modificare la "consistenza" stessa del trattamento (ad es., numero di interessati, tipologia di dati, finalità del trattamento), circostanza difficilmente ipotizzabile senza compromettere le motivazioni stesse alla base dell'ipotesi allo studio della DPIA (ovvero il trattamento stesso, ove già in essere).
La soluzione al problema è agire sul parametro di "probabilità" di accadimento, ovvero ipotizzare contromisure adeguate in base al rischio inerente rilevato.

Le linee guida ENISA suggeriscono un **set di contromisure (tratte dallo standard ISO 27001)** collocandole – in funzione della loro consistenza – in relazione ad uno specifico livello di rischio rilevato. Il quadro delle misure ivi proposte è stato ai fini della presente trattazione semplificato[16] e si è provveduto a verificarne l'aderenza con eventuali standard internazionali e nazionali cogenti o volontari (ad es., linee guida AGID) al fine di verificarne l'effettiva adeguatezza. Naturalmente, alcune delle misure raccomandate potrebbero essere già implementate presso l'organizzazione. Ove così non fosse, **la mancata implementazione configura una vulnerabilità** da gestire mediante un piano di implementazione.
Il set di contromisure di cui è consigliata l'implementazione in funzione del livello di rischio inerente rilevato è riportato in Allegato 3. Per conseguire la scalabilità, si presume che tutte le misure descritte nel livello basso siano applicabili a tutti i livelli. Allo stesso modo, le misure presentate nel livello medio sono applicabili anche ad alto livello di rischio. Le misure presentate nel livello alto (rosso) non sono applicabili a nessun altro livello di rischio.

Il piano di trattamento del rischio dovrebbe essere supportato dalle relative risorse (economiche, organizzative e tecniche) affinché il piano sia effettivamente realizzabile.

La realizzazione del piano è di responsabilità del Delegato del Titolare del trattamento in funzione dell'– ove dotato di specifico budget – ed in coerenza con i limiti di spesa attribuiti, con il supporto del Process Owner e del RPD.
Il piano di trattamento dei rischi concorre, insieme a tutte le altre informazioni legate alle valutazioni preliminari, alla formalizzazione dei risultati della DPIA

## FORMALIZZAZIONE DELLE RISULTANZE DELLA DPIA E CONDIVISIONE CON GLI STAKEHOLDER

Tutta la documentazione prodotta all'interno del processo di DPIA, partendo dal censimento e descrizione del trattamento, passando dalle valutazioni preliminari per arrivare, quando necessario, al calcolo di analisi dei rischi e relativo piano di trattamento, devono concorrere alla realizzazione di un Report finale in grado di dimostrare, oltre ovviamente ai risultati ottenuti, la corretta esecuzione formale del processo e la sua aderenza ai requisiti richiesti dal GDPR.
Il report deve inoltre esplicitare la frequenza di aggiornamento della DPIA, tanto maggiore quanto più si utilizzino tecnologie in evoluzione o si prevedono potenziali variazioni nei processi di trattamento.

L'analisi conclusiva dovrà infine evidenziare se i **livelli di rischio residuo** sono adeguati, in particolare dovrà essere verificato l'allineamento alla propensione al rischio privacy dell'Organizzazione.

Se gli esiti della valutazione DPIA rivelano che il rischio residuo è elevato e non mitigabile (tecnologie e/o costi inapplicabili) occorre consultare l'Autorità di controllo (cfr. par. successivo).

---

[15] cfr. ISO/IEC 31010:2009, Annex B (informative): Risk assessment techniques, punto B.29 "Consequence/probability matrix", pag. 82: "*The format of the matrix and the definitions applied to it depend on the context in which it is used and it is important that an appropriate design is used for the circumstances*".

[16] Ove possibile, in quanto la finalità della presente trattazione non è quella del rispetto dei requisiti ISO ai fini della certificazione

Pur non essendo prevista come obbligatoria[17] una buona prassi potrebbe essere quella di avviare una consultazione pubblica (eventualmente previa comunicazione/pubblicazione di una sintesi della DPIA) al fine di acquisire le **opinioni degli stakeholder esterni (es., PPAA partner in specifici progetti, cluster di interessati)**. Secondo il WP 29, ove il Titolare ritenga di non acquisire tali opinioni o si discosti dalle opinioni formalizzate, dovrebbe documentare le motivazioni alla base della decisione.
Sono invece assolutamente necessari i seguenti passi:

1. richiesta ed acquisizione del **parere finale del RPD** sugli esiti della DPIA; WP29[18] in proposito indica che il parere del RPD dovrebbe riguardare: a) quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate; b) se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al GDPR.
   Anche in questo caso, sempre su indicazione del WP29, ove il Titolare si discosti dal parere formalizzato dal RPD, dovrebbe documentare all'interno della DPIA stessa le motivazioni alla base della decisione
2. previsione nel contratto o atto giuridico analogo dell'eventuale **Responsabile esterno** ex art. 28 del GDPR le misure e gli adempimenti risultati necessari in base alla DPIA, che dovranno essere da questi garantiti
3. rilascio di specifiche **istruzioni ai soggetti interni** ad UC autorizzati a svolgere il trattamento in esame

## CONSULTAZIONE DELL'AUTORITÀ

Qualora:

a) la valutazione d'impatto sulla protezione dei dati a cui si è giunti al termine del processo DPIA e riportato all'interno del Report conclusivo, indichi che il trattamento possa presentare un rischio elevato in assenza di ulteriori misure adottabili dal Titolare del trattamento (ad es., tenendo in considerazione i costi di attuazione), in grado di attenuare il rischio,
b) si ricada nel campo di applicazione dell'art. 36, par. 5 del GDPR, ovvero il diritto interno preveda comunque la consultazione dell'autorità di controllo e/o la sua autorizzazione preliminare, in relazione a trattamenti posti in essere per l'esecuzione di un compito di interesse pubblico

il Titolare del trattamento[19], prima di procedere al trattamento, deve **consultare l'Autorità di Controllo**.

Tale adempimento deve essere considerato parte integrante del processo di DPIA.

A norma dell'art. 36, all'Autorità devono essere comunicate le seguenti informazioni:

- l'allocazione delle responsabilità in capo al titolare, ai contitolari e/o al/ai responsabili del trattamento ove applicabile
- le finalità del trattamento
- i mezzi del trattamento[20]
- le misure e le garanzie previste
- gli esiti finali della DPIA effettuata
- i dati di contatto del RPD
- ogni altra informazione sia nello specifico richiesta dall'autorità di controllo.

Salvo diversa disposizione dell'Autorità Garante è bene che la richiesta di Consultazione avvenga con modalità che consentano di dimostrare la data certa della stessa comunicazione (es. PEC, Raccomandata, ecc.) visto che i tempi stabiliti per lo sviluppo del processo di consultazione preventiva decorreranno da tal data.

L'autorità di controllo può fornire un proprio parere (entro 8 settimane dal ricevimento della richiesta[21]) ove ritenga che il trattamento previsto non sia conforme al GDPR.

Il trattamento oggetto di DPIA **non può essere iniziato** a meno che:

---

[17] cfr. art. 35, par. 9 "se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto"
[18] Cfr. Linee guida sui responsabili della protezione dei dati
[19] Per il tramite del suo delegato *ad acta*, che secondo quanto previsto dal SGDP_ Modello organizzativo, ruoli e sistema di responsabilità di UC è il Presidente di Unioncamere
[20] Per «mezzi del trattamento» devono intendersi: "strumenti tecnici utilizzati per trattare i dati personali (ad es., uno specifico applicativo informatico e le relative misure di sicurezza), ma anche il "come" del trattamento, cioè "quali dati trattare", "chi può avervi accesso", "quanto tempo conservarli ", ecc." (cfr. WP29, Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento")
[21] eventualmente prorogabile – entro il primo mese dal ricevimento della richiesta - di ulteriori 6 settimane sulla base della complessità della trattazione

- il procedimento di consultazione preventiva si sia concluso con successo
- non pervenga alcuna risposta dall'Autorità entro il termine di otto settimane, per cui il silenzio assenso potrà essere interpretato come una implicita conferma che non sono stati ravvisati motivi di contrasto tra il trattamento che si intende iniziare ed il GDPR[22]

## RIESAME DELLA DPIA

La DPIA non è da intendersi come un'attività puntuale da effettuarsi una tantum ma è un processo, un processo che deve essere **ciclicamente attuato e revisionato** tutte le volte che si rende necessario in base ai cambiamenti interni o esterni che si dovessero presentare al trattamento.
Anche la linea guida WP248 sottolinea la necessità di effettuare la DPIA ad intervalli periodici, con una frequenza almeno triennale, anche se non dovessero sopraggiungere cambiamenti apparenti al trattamento.

La revisione della DPIA è necessaria:

a) ove cambino le condizioni di trattamento (ad es., il contesto organizzativo interno, il trattamento, le misure di sicurezza) anche a seguito dell'emersione di diversi o ulteriori profili di rischio (es., data breach, esercizio reiterato dei diritti degli interessati…)
b) per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati

Le attività di trattamento sono verificate periodicamente dal RPD per valutare se queste rispettino le conclusioni della DPIA.

[22] "Se ritiene che il trattamento… violi il presente regolamento… l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento…" cfr. art. 36, par. 2 del GDPR

## MATRICE DELLE RESPONSABILITA'

**Legenda**

- R = Responsabile
- C = Coinvolto
- I = Informato

| *Fase* | *Attività* | *Soggetto/ Struttura* | Dirigente delegato del Titolare | Responsabile della Protezione dei Dati | Presidente Unioncamere | Segretario Generale | Area Legale e Amm.Va | Società esterne Responsabili del trattamento | CED | Altri referenti interni UC |
|---|---|---|---|---|---|---|---|---|---|---|
| ***ANALISI NECESSITÀ DPIA*** | Acquisizione delle informazioni necessarie | | **R** | | | | | | | |
| | Valutazione d'impatto preliminare | | **R** | **C** | | | | | | |
| | Verbalizzazione finale delle risultanze | | **R** | **I** | | **I** | **I** | | | |
| ***CONDUZIONE DPIA*** | Costituzione del Team DPIA | | **R** | | | | **C** | **C** | **C** | **C** |
| | Assegnazione responsabilità interne al Team | | **R** | | | | | | | |
| | Acquisizione degli elementi informativi necessari | | **R** | | | | **C** | **C** | **C** | **C** |
| | Valutazione legittimità e liceità del trattamento | | **R** | **I** | | | **C** | | | |
| | Analisi dei rischi | | **R** | **I** | | | **C** | **C** | **C** | **C** |
| | Definizione contromisure adeguate | | **R** | **C** | | **C** | **I** | **C** | **C** | **C** |
| | Verbalizzazione finale delle risultanze | | **R** | **C** | | **I** | | | | |
| ***FORMALIZZAZIONE DPIA*** | Consultazione stakeholder interni/esterni al Sistema Camerale | | **R** | | | | | | | |
| | Redazione documento finale DPIA | | **R** | **C** | | | | | | |
| | Rilascio istruzioni art. 28 e art. 29 GDPR | | **R** | | | | | | | |
| ***CONSULTAZIONE AUTORITÀ GARANTE*** | Formalizzazione della richiesta di consultazione preliminare all'Autorità Garante | | | **I** | **R** | **I** | | | | |
| | Acquisizione risultanze ed adeguamento (ovvero verifica termine per il silenzio assenso) | | **R** | **I** | **I** | **I** | | | | |
| ***RIESAME PERIODICO DPIA*** | Revisione in caso di cambiamenti interni o esterni al trattamento | | **R** | **C** | | | | | | |

## ALLEGATO 1 – MODELLO ESEMPLIFICATO VALUTAZIONE D'IMPATTO

| | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| 1 | | LIVELLO RILEVATO | CONSISTENZA DEL TRATTAMENTO<br>Il trattamento: | LIVELLO RILEVATO | QUALITA' DEI DATI TRATTATI<br>Il trattamento coinvolge: | LIVELLO RILEVATO | TIPOLOGIA DI INTERESSATI<br>Il trattamento coinvolge: | LIVELLO RILEVATO | TIPOLOGIA DI TRATTAMENTO<br>Il trattamento consiste in: |
| 2 | 1<br>TRASCURABILE | | E' episodico[23] | | Dati identificativi (ad es., anagrafici) | | Nessuna delle ipotesi successive | | Nessuna delle ipotesi successive |
| 3 | 2<br>MEDIO | | Coinvolge un numero limitato (circoscritto) di interessati[24] | | Dati personali elementari (comuni) | | Utenti generici di un servizio | | Acquisizione e gestione di dati attraverso la rete internet |
| 4 | 3<br>MODERATO | | E' svolto in forma strutturata e continuativa come processo di business | | Dati valutativi[25] | | Operatori economici (ditte individuali, professionisti…) | | Trasferimento di dati in paesi o Organizzazioni terzi |
| 5 | 4<br>SIGNIFICATIVO | | E' svolto su larga scala (livello regionale) | | Dati sensibili o dati aventi carattere altamente personale[26] | | Dipendenti<br>Consumatori | | Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative[27]<br>Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione[28]<br>Creazione di corrispondenze o combinazione di insiemi di dati[29] |
| 6 | 5<br>CATASTROFICO | | E' svolto su larga scala (livello nazionale/sovranazionale | | Dati genetici[30]<br>Dati biometrici[31] | | Interessati vulnerabili (es., minori, anziani, portatori di patologie fisiche o mentali, richiedenti asilo…) | | Monitoraggio sistematico[32]<br>Condizionamento degli interessati in relazione all'esercizio dei loro diritti[33]<br>Realizzazione di valutazioni automatiche con effetti giuridici o comunque significativi[34] |

**ALGORITMO DI CALCOLO: =SE(MEDIA(B2:H6)<4;SE(CONTA.SE(B2:H6;">=4")>=2;4;MEDIA(B2:H6));MEDIA(B2:H6))**

[23] numero di interessati limitato/circoscritto (il trattamento di dati non è "sistematico")
[24] ad es., in relazione a funzioni di supporto (risorse umane, acquisti, affari societari...) ovvero a trattamenti/progetti circoscritti sia dal punto di vista temporale che del numero di interessati
[25] Ovvero relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, formulate a partire da dati personali elementari
[26] categorie particolari di dati personali così come definite all'articolo 9, dati personali relativi a condanne penali o reati di cui all'articolo 10; dati personali che consentono la geo-localizzazione (ubicazione); dati relativi alle comunicazioni elettroniche (ad es., indirizzo IP); dati finanziari (situazione economica o patrimoniale, rischio solvibilità, etc.)
[27] Ad es., combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, etc.
[28] 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"
[29] ad esempio, nel caso di interconnessione di banche dati: 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
[30] 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;
[31] 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
[32] 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*"
[33] trattamenti che mirano a consentire, modificare o rifiutare l'esercizio di un diritto degli interessati ovvero l'accesso degli interessati a un servizio oppure la stipula di un contratto.
[34] Decisioni automatizzate con effetti giuridici o che incidano in modo analogo significativamente su persone fisiche

## ALLEGATO 2 – MODELLO DI RILEVAZIONE INFORMAZIONI DPIA

| | |
|---|---|
| **Denominazione DPIA** | |
| **Denominazione del Titolare del trattamento** | |
| Dati di contatto | |
| **Soggetto responsabile della DPIA** | |
| Ruolo del soggetto responsabile | |
| **Responsabile della Protezione dei dati** | |
| Dati di contatto del RPD | |
| | |
| | |

### A) Dati di contesto

Descrizione del trattamento oggetto di DPIA

*(fornire una sintetica descrizione del trattamento/progetto in esame, la sua natura, il contesto di utilizzo, il perimetro geografico di intervento, le finalità, i risultati attesi, le relative problematiche…)*

Responsabilità connesse al trattamento

*(descrivere gli attori coinvolti nel progetto e le relative responsabilità: titolare/contitolari del trattamento, funzioni interne owner del trattamento/progetto, responsabili esterni …)*

Eventuali standard di riferimento applicabili al trattamento

*(elencare le regole o gli standard di riferimento applicabili al trattamento, sia utili sia obbligatori, in particolare i codici di condotta approvati e le certificazioni inerenti la protezione dei dati)*

Qualificazione dei dati personali oggetto di trattamento

*(elencare e qualificare i dati oggetto di raccolta e successivo trattamento, indicando: la tipologia di dati, il numero di "posizioni" – ad es., interessati/eventi – attesi, etc...)*

Ciclo di vita dei dati

*(descrivere il ciclo di vita dei dati – dalla raccolta alla distruzione – servendosi ad es., di un diagramma di flusso e fornendo una dettagliata descrizione in fasi, sottofasi e relative responsabilità ai vari livelli...)*

Risorse a supporto

*(elencare e descrivere le risorse che ospitano i dati o attraverso cui sono gestiti, tra cui ad es.: hardware, software, reti, supporti cartacei o documentazione...)*

**B) Valutazione della liceità del trattamento**

Descrizione delle finalità del trattamento

*(spiegare perché si ritiene che le finalità del trattamento siano specifiche, esplicite e legittime…)*

Basi legali

*(presentare le basi legali del trattamento: ad es., consenso, esecuzione di un contratto, obbligo legale, interesse pubblico, etc…)*

Minimizzazione dei dati

*(analizzare perché si ritiene che i dati raccolti siano adeguati, pertinenti e limitati a quanto è necessario sulla base delle finalità del trattamento…)*

Esattezza ed aggiornamento dei dati

*(descrivere le misure previste per garantire la qualità dei dati…)*

Conservazione dei dati

*(indicare il periodo di conservazione e le modalità/ragioni della scelta: ad es., obbligo di legge ovvero, in caso contrario, perché il periodo di retention autonomamente definito sia necessario al raggiungimento delle finalità del trattamento…)*

Informazione e trasparenza

*(descrivere le informazioni che si prevede di fornire agli interessati e gli strumenti utilizzati a tale scopo…)*

Consenso dell'interessato

*(ove applicabile in relazione alla base giuridica utilizzata, descrivere le modalità previste per ottenere e documentare il consenso degli interessati…)*

Esercizio dei diritti

*(descrivere quali diritti – evidenziando e giustificando eventuali limitazioni – sono esercitabili e le modalità tecniche, organizzative e/o gestionali volte a consentire agli interessati di esercitarli…)*

Definizione delle responsabilità esterne

*(ove applicabile, in caso di contitolarità o di outsourcing, descrivere l'ambito di rispettiva responsabilità sui dati personali ed i riferimenti contrattuali - contratto o altro atto analogo - in cui tali aspetti sono regolamentati…)*

Trasferimenti in paesi terzi

*(ove applicabile, indicare il Paese o l'organizzazione internazionale di destinazione dei dati e le cautele adottate: ad es., valutazione di adeguatezza, clausole contrattuali standard, BCR…)*

## ALLEGATO 3 – MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

### POLITICA DI SICUREZZA E PROCEDURE PER LA PROTEZIONE DEI DATI PERSONALI

| Misura | Rif. standard | Livello di rischio rilevato |
|---|---|---|
| L'organizzazione dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni. | ISO IEC 27001:2013 (A.5)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 24 e 32)<br>D.Lgs. 196/2003 e s.m.i. (art. 2-quaterdecies) | Basso |
| La politica di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale. | ISO IEC 27001:2013 (A.5)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i. (-) | Basso |
| L'organizzazione dovrebbe documentare una policy di sicurezza dedicata separata per quanto riguarda il trattamento dei dati personali. La policy deve essere approvata dal management competente e comunicata a tutti i dipendenti, persone autorizzate al trattamento e alle parti esterne interessate | ISO IEC 27001:2013 (A.5)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i. (-) | Medio |
| La policy di sicurezza dovrebbe almeno riferirsi a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, i responsabili del trattamento dei dati o altre terze parti coinvolte nel trattamento dei dati personali. | ISO IEC 27001:2013 (A.5)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i. (-) | Medio |
| Dovrebbe essere creato e mantenuto un inventario di policy / procedure specifiche relative alla sicurezza dei dati personali, basato sulla policy generale di sicurezza. | ISO IEC 27001:2013 (A.5)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i. (-) | Medio |
| Le policy di sicurezza dovrebbero essere riviste e corrette, se necessario, su base semestrale. | ISO IEC 27001:2013 (A.5)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 32, 1, lett. d)<br>D.Lgs. 196/2003 e s.m.i. (-) | Alto |

### RUOLI E RESPONSABILITA'

| Misura | Rif. standard | Livello di rischio rilevato |
|---|---|---|
| I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con le politiche di sicurezza. | ISO IEC 27001:2013 (A.6.1.1)<br>Circolare Agid 2/2017 (-)<br>GDPR (artt. 28 e 29)<br>D.Lgs. 196/2003 e s.m.i. (art. 2-quaterdecies) | Basso |
| In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo, l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento (es. laptop, tablet, smartphone, hd esterni/pen drive…) | ISO IEC 27001:2013 (A.6.1.1)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 32)<br>D.Lgs. 196/2003 e s.m.i. (art. 2-quaterdecies) | Basso |
| Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza. | ISO IEC 27001:2013 (A.6.1.1)<br>Circolare Agid 2/2017 (5.1.1, 5.2.1)<br>GDPR (artt. 28 e 29)<br>D.Lgs. 196/2003 e s.m.i. (art. 2-quaterdecies)<br>Garante Privacy (provv. 27/11/2008) | Medio |
| Il responsabile della sicurezza dovrebbe essere nominato formalmente (documentato). Anche i compiti e le responsabilità del responsabile della sicurezza dovrebbero essere chiaramente definiti e documentati. | ISO IEC 27001:2013 (A.6.1.1)<br>Circolare Agid 2/2017 (5.1.1, 5.2.1) | Alto |

| | | |
|---|---|---|
| | GDPR (artt. 28 e 29)<br>D.Lgs. 196/2003 e s.m.i. (art. 2-quaterdecies)<br>Garante Privacy (provv. 27/11/2008) | |
| Compiti e responsabilità in conflitto, ad esempio i ruoli di responsabile della sicurezza, revisore della sicurezza e DPO, dovrebbero essere considerati separatamente per ridurre le ipotesi di modifiche non autorizzate o non intenzionali o un uso improprio di dati personali | ISO IEC 27001:2013 (A.6.1.1)<br>Circolare Agid 2/2017 (5.10.1)<br>GDPR (art. 24)<br>D.Lgs. 196/2003 e s.m.i. (art. 2-quaterdecies)<br>WP 243 del 05/04/2017 | Alto |
| **POLITICHE DI CONTROLLO ACCESSI** | | |
| Misura | Rif. standard | Livello di rischio rilevato |
| I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati. | ISO IEC 27001:2013 (A.9.1.1)<br>Circolare Agid 2/2017 (5.1.1, 5.10.1)<br>GDPR (art. 32, par. 1, lett. b)<br>D.Lgs. 196/2003 e s.m.i. (-) | Basso |
| Dovrebbe essere dettagliata e documentata una politica di controllo degli accessi. L'organizzazione dovrebbe determinare in questo documento le regole di controllo appropriate degli accessi, i diritti di accesso e le restrizioni per specifici ruoli degli utenti nell'ambito dei processi e delle procedure relative ai dati personali. | ISO IEC 27001:2013 (A.9.1.1)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 32, par. 1, lett. b e d)<br>D.Lgs. 196/2003 e s.m.i. (-) | Medio |
| Dovrebbe essere chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi). | ISO IEC 27001:2013 (A.9.1.1)<br>Circolare Agid 2/2017 (5.1.1-5.1.2)<br>GDPR (art. 32, par. 1, lett. b)<br>D.Lgs. 196/2003 e s.m.i. (-)<br>Garante Privacy (provv. 27/11/2008) | Medio |
| I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff | ISO IEC 27001:2013 (A.9.1.1)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 32, par. 1, lett. b)<br>D.Lgs. 196/2003 e s.m.i. (-) | Alto |
| **GESTIONE RISORSE/ASSET** | | |
| Misura | Rif. standard | Livello di rischio rilevato |
| L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT). | ISO IEC 27001:2013 (A.8)<br>Circolare Agid 2/2017 (1.1.1-1.6.1 e 2.1.1-2.4.1)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i. (-) | Basso |
| Il censimento delle risorse e degli apparati IT e il relativo registro dovrebbero essere rivisti e aggiornati regolarmente. | ISO IEC 27001:2013 (A.8)<br>Circolare Agid 2/2017 (1.3.2, 1.3.3)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i. (-) | Medio |
| I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati. | ISO IEC 27001:2013 (A.8)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i. (-) | Medio |
| Le risorse IT dovrebbero essere riviste e aggiornate su base annuale. | ISO IEC 27001:2013 (A.8)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i. (-) | Alto |

| GESTIONE DELLE MODIFICHE APPORTATE ALLE RISORSE, AGLI APPARATI ED AI SISTEMI IT | | |
|---|---|---|
| Misura | Rif. standard | Livello di rischio rilevato |
| L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica. | ISO IEC 27001:2013 (A.12.1)<br>Circolare Agid 2/2017 (3.2.3, 3.6.1)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i. (-) | Basso |
| Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software. | ISO IEC 27001:2013 (A.12.1)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i. (-) | Basso |
| Dovrebbe essere prevista e applicata una policy interna che disciplini la gestione delle modifiche e che includa per lo meno: un processo che governi l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche dovrebbe essere regolarmente aggiornata. | ISO IEC 27001:2013 (A.12.1)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i. (-) | Medio |
| RESPONSABILI DEL TRATTAMENTO | | |
| Misura | Rif. Standard | Livello di rischio rilevato |
| Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento. | ISO IEC 27001:2013 (A.15)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 28)<br>D.Lgs. 196/2003 e s.m.i. (-) | Basso |
| Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi. | ISO IEC 27001:2013 (A.15)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 28, par. 3 lett. f)<br>D.Lgs. 196/2003 e s.m.i. (-) | Basso |
| Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza. | ISO IEC 27001:2013 (A.15)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 28, par. 1)<br>D.Lgs. 196/2003 e s.m.i. (-) | Basso |
| L'organizzazione del titolare del trattamento dovrebbe svolgere regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi. | ISO IEC 27001:2013 (A.15)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 28, par. 3, lett. h)<br>D.Lgs. 196/2003 e s.m.i. (-) | Medio |
| I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi documentati di riservatezza / non divulgazione. | ISO IEC 27001:2013 (A.15)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 28, par. 3, lett. b)<br>D.Lgs. 196/2003 e s.m.i. (-) | Alto |
| GESTIONE DEGLI INCIDENTI / VIOLAZIONE DEI DATI PERSONALI (PERSONAL DATA BREACHES) | | |
| Misura | Rif. standard | Livello di rischio rilevato |
| È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali. | ISO IEC 27001:2013 (A.16)<br>Circolare Agid 2/2017 (-)<br>GDPR (artt. 33 e 34)<br>D.Lgs. 196/2003 e s.m.i. (-) | Basso |
| Le violazioni dei dati personali (come definite dall'art. 4 del GDPR) devono essere segnalate immediatamente al | ISO IEC 27001:2013 (A.16) | Basso |

| | | |
|---|---|---|
| Management competente secondo l'organizzazione interna. Dovrebbero essere in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi degli art. 33 e 34 GDPR. | Circolare Agid 2/2017 (-)<br>GDPR (artt. 33 e 34)<br>D.Lgs. 196/2003 e s.m.i. (-) | |
| L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali). | ISO IEC 27001:2013 (A.16)<br>Circolare Agid 2/2017 (-)<br>GDPR (artt. 33 e 34, art. 32, par. 1, lett. b e c)<br>D.Lgs. 196/2003 e s.m.i. (-) | Basso |
| Il piano di risposta degli incidenti (Incident Response Plan) dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli. | ISO IEC 27001:2013 (A.16)<br>Circolare Agid 2/2017 (-)<br>GDPR (artt. 33 e 34, art. 32, par. 1, lett. b e c)<br>D.Lgs. 196/2003 e s.m.i. (-) | Medio |
| Gli incidenti e le violazioni dei dati personali devono essere registrati insieme ai dettagli riguardanti l'evento e le successive azioni di mitigazione intraprese | ISO IEC 27001:2013 (A.16)<br>Circolare Agid 2/2017 (4.2.1-4.2.3)<br>GDPR (artt. 33 e 34, art. 32, par. 1, lett. b e c)<br>D.Lgs. 196/2003 e s.m.i. (-) | Alto |
| **BUSINESS CONTINUITY** | | |
| Misura | Rif. standard | Livello di rischio rilevato |
| L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali). | ISO IEC 27001:2013 (A.17)<br>Circolare Agid 2/2017 (-)<br>GDPR (artt. 33 e 34; art. 32, par. 1, lett. b e c)<br>D.Lgs. 196/2003 e s.m.i. (-) | Basso |
| Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli. | ISO IEC 27001:2013 (A.17)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 32, par. 1, lett. b e c)<br>D.Lgs. 196/2003 e s.m.i. (-) | Medio |
| Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi aziendali fondamentali che attengono alla sicurezza dei dati personali. | ISO IEC 27001:2013 (A.17)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 32, par. 1, lett. b e c)<br>D.Lgs. 196/2003 e s.m.i. (-) | Medio |
| Dovrebbe essere nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati personali. | ISO IEC 27001:2013 (A.17)<br>Circolare Agid 2/2017 (-)<br>GDPR (artt. 28 e 29; art. 32, par. 1, lett. b e c)<br>D.Lgs. 196/2003 e s.m.i. (art. 2-quaterdecies) | Alto |
| Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT | ISO IEC 27001:2013 (A.17)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 32, par. 1, lett. b e c)<br>D.Lgs. 196/2003 e s.m.i. (-) | Alto |
| **OBBLIGHI DI CONFIDENZIALITÀ** | | |
| Misura | Rif. standard | Livello di rischio rilevato |
| L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti, assegnati e comunicati durante il processo di pre-assunzione e / o assunzione . | ISO IEC 27001:2013 (A.7)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 29)<br>D.Lgs. 196/2003 e s.m.i. (art. 2-quaterdecies) | Basso |
| Prima di assumere i propri compiti, i dipendenti, lavoratori e persone autorizzate al trattamento dovrebbero essere invitati a rivedere e concordare le policy di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e | ISO IEC 27001:2013 (A.7)<br>Circolare Agid 2/2017 (-) | Medio |

| | | |
|---|---|---|
| di non divulgazione. | GDPR (art. 29)<br>D.Lgs. 196/2003 e s.m.i. (art. 2-quaterdecies) | |
| I dipendenti coinvolti nel trattamento dei dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale) | ISO IEC 27001:2013 (A.7)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 29)<br>D.Lgs. 196/2003 e s.m.i. (art. 2-quaterdecies) | Alto |
| **FORMAZIONE** | | |
| Misura | Rif. standard | Livello di rischio rilevato |
| L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica. | ISO IEC 27001:2013 (A.7.2.2)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 29)<br>D.Lgs. 196/2003 e s.m.i. (art. 2-quaterdecies) | Basso |
| L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici per l'introduzione (alle questioni di protezione dei dati) dei nuovi arrivati. | ISO IEC 27001:2013 (A.7.2.2)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 29)<br>D.Lgs. 196/2003 e s.m.i. (art. 2-quaterdecies) | Medio |
| Dovrebbe essere predisposto ed eseguito su base annuale un piano di formazione con scopi e obiettivi definiti. | ISO IEC 27001:2013 (A.7.2.2)<br>Circolare Agid 2/2017 (<br>GDPR (art. 29)<br>D.Lgs. 196/2003 e s.m.i. (art. 2-quaterdecies) | Alto |
| **CONTROLLO DEGLI ACCESSI E AUTENTICAZIONE** | | |
| Misura | Rif. standard | Livello di rischio rilevato |
| Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente. | ISO IEC 27001:2013 (A.9)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 32, par. 1, lett. b)<br>D.Lgs. 196/2003 (-) | Basso |
| L'uso di account utente comuni (con credenziali di accesso condivise tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità | ISO IEC 27001:2013 (A.9)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 32, par. 1, lett. b)<br>D.Lgs. 196/2003 (-) | Basso |
| Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità. | ISO IEC 27001:2013 (A.9)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 32, par. 1, lett. b)<br>D.Lgs. 196/2003 (-) | Basso |
| Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile). | ISO IEC 27001:2013 (A.9)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 32, par. 1, lett. b)<br>D.Lgs. 196/2003 (-) | Basso |
| Dovrebbe essere definita e documentata una policy specifica per la password. La policy deve includere almeno la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili. | ISO IEC 27001:2013 (A.9)<br>Circolare Agid 2/2017 (<br>GDPR (art. 32, par. 1, lett. b)<br>D.Lgs. 196/2003(-) | Medio |
| Le password degli utenti devono essere memorizzate in una forma "hash" | ISO IEC 27001:2013 (A.9)<br>Circolare Agid 2/2017 (-) | Medio |

| | | |
|---|---|---|
| | GDPR (art. 32, par. 1, lett. b)<br>D.Lgs. 196/2003 (-) | |
| L'autenticazione a due fattori (autenticazione forte) dovrebbe preferibilmente essere implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc. | ISO IEC 27001:2013 (A.9)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 32, par. 1, lett. b)<br>D.Lgs. 196/2003 (-) | Alto |
| Dovrebbe essere un soggetto ad autenticazione ogni dispositivo (autenticazione endpoint) per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale | ISO IEC 27001:2013 (A.9)<br>Circolare Agid 2/2017 (1.5.1 e 1.6.1)<br>GDPR (-)<br>D.Lgs. 196/2003 (-) | Alto |

## GENERAZIONE DI FILE DI LOG E MONITORAGGIO

| Misura | Rif. standard | Livello di rischio rilevato |
|---|---|---|
| Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione). | ISO IEC 27001:2013 (A.12.4)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 (-) | Basso |
| I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento | ISO IEC 27001:2013 (A.12.4)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 (-) | Basso |
| Dovrebbe essere necessario registrare le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente | ISO IEC 27001:2013 (A.12.4)<br>Circolare Agid 2/2017 (5.1.4, 5.4.1-5.5.1)<br>GDPR (-)<br>D.Lgs. 196/2003 (-)<br>Garante Privacy (provv. 27/11/2008) | Medio |
| Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. Anche l'accesso ai file di registro dovrebbe essere registrato oltre al monitoraggio per rilevare attività insolite | ISO IEC 27001:2013 (A.12.4)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 (-)<br>Garante Privacy (provv. 27/11/2008) | Medio |
| Un sistema di monitoraggio dovrebbe generare i file log e produrre report sullo stato del sistema e notificare potenziali allarmi | ISO IEC 27001:2013 (A.12.4)<br>Circolare Agid 2/2017 (-)<br>GDPR (artt. 33 e 34)<br>D.Lgs. 196/2003 (-)<br>Garante Privacy (provv. 27/11/2008) | Medio |

## SICUREZZA DI SERVER E DATABASE

| Misura | Rif. standard | Livello di rischio rilevato |
|---|---|---|
| I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente | ISO IEC 27001:2013 (A.12)<br>Circolare Agid 2/2017 (5.1.2,<br>GDPR (-)<br>D.Lgs. 196/2003(-) | Basso |
| I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate | ISO IEC 27001:2013 (A.12)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 5, par. 1, lett. c)<br>D.Lgs. 196/2003(-) | Basso |

| | | |
|---|---|---|
| Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware. | ISO IEC 27001:2013 (A.12)<br>Circolare Agid 2/2017 (13.1.1-13.2.1)<br>GDPR (art. 32, par. 1, lett. a)<br>D.Lgs. 196/2003(-) | Medio |
| Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione. | ISO IEC 27001:2013 (A.12)<br>Circolare Agid 2/2017 (13.1.1-13.2.1)<br>GDPR (art. 32, par. 1, lett. a)<br>D.Lgs. 196/2003 (-) | Medio |
| Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato senza ulteriori informazioni | ISO IEC 27001:2013 (A.12)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 32, 1, lett. a)<br>D.Lgs. 196/2003 (-) | Medio |
| Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della privacy, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc. | SO IEC 27001:2013 (A.12)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 25)<br>D.Lgs. 196/2003 (-) | Alto |
| SICUREZZA DELLE POSTAZIONI DI LAVORO | | |
| Misura | Rif. standard | Livello di rischio rilevato |
| Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza. | ISO IEC 27001:2013 (A.14.1)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 (-) | Basso |
| Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale. | ISO IEC 27001:2013 (A.14.1)<br>Circolare Agid 2/2017 (8.1.1)<br>GDPR (-)<br>D.Lgs. 196/2003 (-) | Basso |
| Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate. | ISO IEC 27001:2013 (A.14.1)<br>Circolare Agid 2/2017 (2.1.1, 5.1.1, 8.9.3)<br>GDPR (-)<br>D.Lgs. 196/2003 (-) | Basso |
| Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo. | ISO IEC 27001:2013 (A.14.1)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 (-) | Basso |
| Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente. | ISO IEC 27001:2013 (A.14.1)<br>Circolare Agid 2/2017 (4.5.1, 4.8.2)<br>GDPR (-)<br>D.Lgs. 196/2003 (-) | Basso |
| Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera. | ISO IEC 27001:2013 (A.14.1)<br>Circolare Agid 2/2017 (8.1.1)<br>GDPR (-)<br>D.Lgs. 196/2003 (-) | Medio |
| Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni) | ISO IEC 27001:2013 (A.14.1)<br>Circolare Agid 2/2017 (8.3.1-8.6.1, 13.5.1)<br>GDPR (-) | Alto |

| | | |
|---|---|---|
| | D.Lgs. 196/2003 (-) | |
| Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali. | ISO IEC 27001:2013 (A.14.1)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 (-) | Alto |
| La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro | ISO IEC 27001:2013 (A.14.1)<br>Circolare Agid 2/2017 (13.1.1-13.3.1)<br>GDPR (art. 32, par. 1, lett. a)<br>D.Lgs. 196/2003 (-) | Alto |
| **SICUREZZA DELLA RETE E DELLE INFRASTRUTTURE DI COMUNICAZIONE ELETTRONICA** | | |
| Misura | Rif. standard | Livello di rischio rilevato |
| Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL). | ISO IEC 27001:2013 (A.13)<br>Circolare Agid 2/2017 (13.1.1)<br>GDPR (art. 32, par. 1, lett. a)<br>D.Lgs. 196/2003 (-) | Basso |
| L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia | ISO IEC 27001:2013 (A.13)<br>Circolare Agid 2/2017 (13.1.1)<br>GDPR (art. 32, par. 1, lett. a)<br>D.Lgs. 196/2003(-) | Medio |
| In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti. | ISO IEC 27001:2013 (A.13)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003(-) | Medio |
| Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni. | ISO IEC 27001:2013 (A.13)<br>Circolare Agid 2/2017 (8.1.2, 13.6.2-13.8.1)<br>GDPR (art. 32, par. 1, lett. b)<br>D.Lgs. 196/2003(-) | Medio |
| La connessione a Internet non dovrebbe essere consentita ai server e alle postazioni di lavoro utilizzate per il trattamento dei dati personali | ISO IEC 27001:2013 (A.13)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003(-) | Alto |
| La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati | ISO IEC 27001:2013 (A.13)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 (-) | Alto |
| L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC) | ISO IEC 27001:2013 (A.13)<br>Circolare Agid 2/2017 (1.5.1, 8.3.1)<br>GDPR (-)<br>D.Lgs. 196/2003(-) | Alto |
| **BACK-UP** | | |
| Misura | Rif. standard | Livello di rischio rilevato |
| Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità. | ISO IEC 27001:2013 (A.12.3)<br>Circolare Agid 2/2017 (10.1.1-10.4.1)<br>GDPR (art. 32, par. 1, lett. b e c)<br>D.Lgs. 196/2003 (-) | Basso |

| | | |
|---|---|---|
| Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine. | ISO IEC 27001:2013 (A.12.3)<br>Circolare Agid 2/2017 (10.3.1)<br>GDPR (art. 32, par. 1, lett. b e c)<br>D.Lgs. 196/2003 (-) | Basso |
| L'esecuzione dei backup deve essere monitorata per garantirne la completezza. | ISO IEC 27001:2013 (A.12.3)<br>Circolare Agid 2/2017 (10.2.1)<br>GDPR (art. 32, par. 1, lett. b e c)<br>D.Lgs. 196/2003 (-) | Basso |
| I backup completi devono essere eseguiti regolarmente. | ISO IEC 27001:2013 (A.12.3)<br>Circolare Agid 2/2017 (10.1.1)<br>GDPR (art. 32, par. 1, lett. b e c)<br>D.Lgs. 196/2003 e s.m.i. (-) | Basso |
| I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza. | ISO IEC 27001:2013 (A.12.3)<br>Circolare Agid 2/2017 (10.2.1)<br>GDPR (art. 32, par. 1, lett. b e c)<br>D.Lgs. 196/2003 e s.m.i. (-) | Medio |
| I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera | ISO IEC 27001:2013 (A.12.3)<br>Circolare Agid 2/2017 (10.1.1)<br>GDPR (art. 32, par. 1, lett. b e c)<br>D.Lgs. 196/2003 e s.m.i.(-) | Medio |
| Le copie del backup devono essere conservate in modo sicuro in luoghi diversi. | ISO IEC 27001:2013 (A.12.3)<br>Circolare Agid 2/2017 (10.1.3, 10.4.1)<br>GDPR (art. 32, par. 1, lett. b e c)<br>D.Lgs. 196/2003 e s.m.i.(-) | Medio |
| Se viene utilizzato un servizio di terze parti per l'archiviazione di backup, la copia deve essere crittografata prima di essere trasmessa dal titolare del trattamento | ISO IEC 27001:2013 (A.12.3)<br>Circolare Agid 2/2017 (10.3.1)<br>GDPR (art. 32, par. 1, lett. b e c)<br>D.Lgs. 196/2003 e s.m.i.(-) | Medio |
| Le copie dei backup dovrebbero essere crittografate e archiviate in modo sicuro, anche offline | ISO IEC 27001:2013 (A.12.3)<br>Circolare Agid 2/2017 (10.3.1-10.4.1)<br>GDPR (art. 32, par. 1, lett. b e c)<br>D.Lgs. 196/2003 e s.m.i. (-) | Alto |
| SICUREZZA DEL CICLO DI VITA DELLE APPLICAZIONI | | |
| Misura | Rif. standard | Livello di rischio rilevato |
| Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti. | ISO IEC 27001:2013 (A.12.6, A14.2)<br>Circolare Agid 2/2017 (-)<br>GDPR (artt. 25, 35 e 36)<br>D.Lgs. 196/2003 e s.m.i.(-) | Basso |
| Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo. | ISO IEC 27001:2013 (A.12.6, A14.2)<br>Circolare Agid 2/2017 (-)<br>GDPR (artt. 25, 35 e 36)<br>D.Lgs. 196/2003 e s.m.i.(-) | Basso |
| Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza. | ISO IEC 27001:2013 (A.12.6, A14.2)<br>Circolare Agid 2/2017 (-)<br>GDPR (-) | Basso |

| | | |
|---|---|---|
| | D.Lgs. 196/2003 e s.m.i.(-) | |
| Dovrebbero essere seguiti standard e pratiche di codifica sicure. | ISO IEC 27001:2013 (A.12.6, A14.2)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 25)<br>D.Lgs. 196/2003 e s.m.i.(-) | Basso |
| Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali. | ISO IEC 27001:2013 (A.12.6, A14.2)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 25)<br>D.Lgs. 196/2003 e s.m.i.(-) | Basso |
| Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture dovrebbero essere eseguiti da una terza parte certificata prima dell'adozione operativa. L'applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto. | ISO IEC 27001:2013 (A.12.6, A14.2)<br>Circolare Agid 2/2017 (4.1.1-4.10.1)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i. (-) | Medio |
| Devono essere eseguiti test periodici di penetrazione | ISO IEC 27001:2013 (A.12.6, A14.2)<br>Circolare Agid 2/2017 (4.1.1-4.10.1)<br>GDPR (art. 32, par. 1, lett. d)<br>D.Lgs. 196/2003 e s.m.i.(-) | Medio |
| Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati. | ISO IEC 27001:2013 (A.12.6, A14.2)<br>Circolare Agid 2/2017 (4.1.1-4.10.1.)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i.(-) | Medio |
| I patch software dovrebbero essere testati e valutati prima di essere installati in un ambiente operativo. | ISO IEC 27001:2013 (A.12.6, A14.2)<br>Circolare Agid 2/2017 (4.1.1-4.10.1.)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i.(-) | Medio |
| CANCELLAZIONE / ELIMINAZIONE DEI DATI | | |
| Misura | Rif. standard | Livello di rischio rilevato |
| La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica. | ISO IEC 27001:2013 (A.8.3.2, A.11.2.7)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i.(-)<br>Garante Privacy (provv. 13/10/2008) | Basso |
| È necessario eseguire la triturazione della carta e dei supporti portatili utilizzati per memorizzare i dati personali. | ISO IEC 27001:2013 (A.8.3.2, A.11.2.7)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i.(-) | Basso |
| Più passaggi di sovrascrittura basata su software devono essere eseguiti su tutti i supporti prima di essere smaltiti. | ISO IEC 27001:2013 (A.8.3.2, A.11.2.7)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i.(-)<br>Garante Privacy (provv. 13/10/2008) | Medio |
| Se i servizi di terzi sono utilizzati per disporre in modo sicuro di supporti o documenti cartacei, è necessario stipulare un contratto di servizio e produrre un record di distruzione dei record, a seconda dei casi. | ISO IEC 27001:2013 (A.8.3.2, A.11.2.7)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 28)<br>D.Lgs. 196/2003 e s.m.i.(-) | Medio |

| | | |
|---|---|---|
| Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica. | ISO IEC 27001:2013 (A.8.3.2, A.11.2.7)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i.(-)<br>Garante Privacy (provv. 13/10/2008) | Alto |
| Se è una terza parte, (quindi un responsabile del trattamento) ad occuparsi della distruzione di supporti o file cartacei, il processo si dovrebbe svolgere presso le sedi del titolare del trattamento (ed evitare il trasferimento all'esterno dei dati personali). | ISO IEC 27001:2013 (A.8.3.2, A.11.2.7)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 28)<br>D.Lgs. 196/2003 e s.m.i.(-)<br>Garante Privacy (provv. 13/10/2008) | Alto |
| **SICUREZZA FISICA** | | |
| Misura | Rif. standard | Livello di rischio rilevato |
| Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile da personale non autorizzato. | ISO IEC 27001:2013 (A.11)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i.(-) | Basso |
| Identificazione chiara, tramite mezzi appropriati, ad es. badge identificativi, per tutto il personale e i visitatori che accedono ai locali dell'organizzazione, dovrebbero essere stabiliti, a seconda dei casi. | ISO IEC 27001:2013 (A.11)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i.(-) | Medio |
| Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Un registro fisico o una traccia elettronica di controllo di tutti gli accessi dovrebbero essere mantenuti e monitorati in modo sicuro | ISO IEC 27001:2013 (A.11)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i.(-) | Medio |
| I sistemi di rilevamento anti-intrusione dovrebbero essere installati in tutte le zone di sicurezza | ISO IEC 27001:2013 (A.11)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i.(-) | Medio |
| Se del caso, dovrebbero essere costruite barriere fisiche per impedire l'accesso fisico non autorizzato | ISO IEC 27001:2013 (A.11)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i.(-) | Medio |
| Un sistema antincendio automatico, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di continuità (UPS) dovrebbero essere attivati nella sala server | ISO IEC 27001:2013 (A.11)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i.(-) | Medio |
| Il personale di servizio di supporto esterno deve avere accesso limitato alle aree protette. | ISO IEC 27001:2013 (A.11)<br>Circolare Agid 2/2017 (-<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i. (-) | Medio |
| **DISPOSITIVI MOBILI / PORTATILI** | | |
| Misura | Rif. standard | Livello di rischio rilevato |
| Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo | ISO IEC 27001:2013 (A.6.2)<br>Circolare Agid 2/2017 (-)<br>GDPR (-) | Basso |

| | | |
|---|---|---|
| | D.Lgs. 196/2003 e s.m.i.(-) | |
| I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e preautorizzati | ISO IEC 27001:2013 (A.6.2)<br>Circolare Agid 2/2017 (1.1.1 e 1.5.1)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i.(-) | Basso |
| I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali | ISO IEC 27001:2013 (A.6.2)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 32, par. 1, lett. b)<br>D.Lgs. 196/2003 e s.m.i.(-) | Basso |
| I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti | ISO IEC 27001:2013 (A.6.2)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i.(-) | Medio |
| L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile che è stato compromesso. | ISO IEC 27001:2013 (A.6.2)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i.(-) | Medio |
| I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri. | ISO IEC 27001:2013 (A.6.2)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i.(-) | Medio |
| I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso. | ISO IEC 27001:2013 (A.6.2)<br>Circolare Agid 2/2017 (-)<br>GDPR (-)<br>D.Lgs. 196/2003 e s.m.i. (-) | Medio |
| Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte) | ISO IEC 27001:2013 (A.6.2)<br>Circolare Agid 2/2017 (-)<br>GDPR (art. 32, par. 1, lett. b)<br>D.Lgs. 196/2003 e s.m.i. (-) | Alto |
| I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati. | ISO IEC 27001:2013 (A.6.2)<br>Circolare Agid 2/2017 (13.1.1.)<br>GDPR (art. 32, par. 1, lett. a)<br>D.Lgs. 196/2003 e s.m.i. | Alto |

ALLEGATO 4

UNIONCAMERE

# SGDP - SISTEMA DI GESTIONE DEI DATI PERSONALI
# Procedura di gestione delle richieste di esercizio dei diritti degli interessati

ai sensi del Regolamento UE 679/2016

## SOMMARIO

# PREMESSA

## SCOPO E CAMPO DI APPLICAZIONE

Scopo della presente procedura è descrivere le attività relative al processo di evasione delle richieste di esercizio dei diritti da parte degli interessati.

Tale processo regolamenta le fasi di ricezione, istruttoria e formalizzazione del riscontro agli interessati nonché le modalità per la tenuta di idonee registrazioni per documentare il rispetto degli obblighi imposti nel rispetto del principio di accountability.

La presente procedura è portata a conoscenza, anche attraverso attività di sensibilizzazione o formazione, di tutti i Dirigenti, Quadri, funzionari o, comunque, referenti delle Aree/Uffici di Unioncamere potenzialmente coinvolti nella stessa.

## RIFERIMENTI NORMATIVI

La presente procedura risponde ai seguenti requisiti normativi:

1. Diritti dell'interessato (CAPO III - artt. 12 e ss. GDPR)
2. Codice della privacy (D.lgs. n. 196/2003)

## ACRONIMI E DEFINIZIONI UTILIZZATE

| | |
|---|---|
| GDPR | Regolamento UE 2016/679 (General Data Protection Regulation) |
| Codice | D.Lgs. 196/2003 “Codice in materia di protezione dei dati personali” come modificato dal D.Lgs. 101/2018 |
| Garante | Garante per la protezione dei dati personali |
| RPD | Responsabile della protezione dei dati |
| Delegato del Titolare | Soggetto che, secondo le deleghe/procure formalizzate ed il sistema di gestione della privacy, garantisce specifiche funzioni ai fini della *compliance* al GDPR |
| SG | Segretario Generale di Unioncamere |
| | |
| | |
| | |
| | |
| | |
| | |

## MATRICE DELLA REDAZIONE E DELLE REVISIONI

| Data | Stato | Descrizione | Approvazione |
|---|---|---|---|
| 13/12/2018 | Approvato | Rev 0 – I[a] emissione | Delibera del Comitato esecutivo del 13/12/2018 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## I DIRITTI DEGLI INTERESSATI

Com'è noto, gli interessati[1] possono esercitare, ai sensi degli artt. 15 e ss. del GDPR con riferimento ai propri dati personali eventualmente detenuti da Unioncamere, i seguenti diritti:

1. **Diritto di accesso** > accedere ai dati e ottenerne una copia e, inoltre, essere informati su finalità del trattamento, categorie di dati, destinatari, il periodo per il quale i dati saranno archiviati;
2. **Diritto di rettifica** > ottenere che i dati inesatti o incompleti siano modificati o completati;
3. **Diritto alla cancellazione** (oblio) > far cancellare tutti i dati, link, copia e riproduzione (se diffusi pubblicamente);
4. **Diritto di opposizione** > opporsi al trattamento dei dati, per es. per finalità specifiche come il trattamento per finalità di marketing;
5. **Diritto alla limitazione** > a determinate condizioni, contrassegnare i dati al fine di limitare il loro trattamento, in particolare spostando i dati per renderli non disponibili, per es. in caso di contestazione dell'accuratezza dei dati o se questi vengono conservati solo a scopo di prova in caso di contenzioso;
6. **Diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato** > opposizione ad un trattamento derivante esclusivamente da dati derivati o dedotti, per es. artificialmente generati attraverso algoritmi;
7. **Diritto alla portabilità** > diritto di ricevere i dati trattati con strumenti automatizzati in un formato digitale comunemente utilizzato e leggibile e diritto di richiedere di trasmettere tali dati a un altro titolare (ove possibile).

In merito al corretto inquadramento dei diritti esercitabili, si rinvia alle FAQ di cui all'All. 1.

In proposito si deve specificare che l'esercizio dei diritti deve essere richiesto al **Titolare del trattamento**, il quale è obbligato a darvi seguito, non potendo riversare tali adempimenti in capo ad altri soggetti. Quindi:

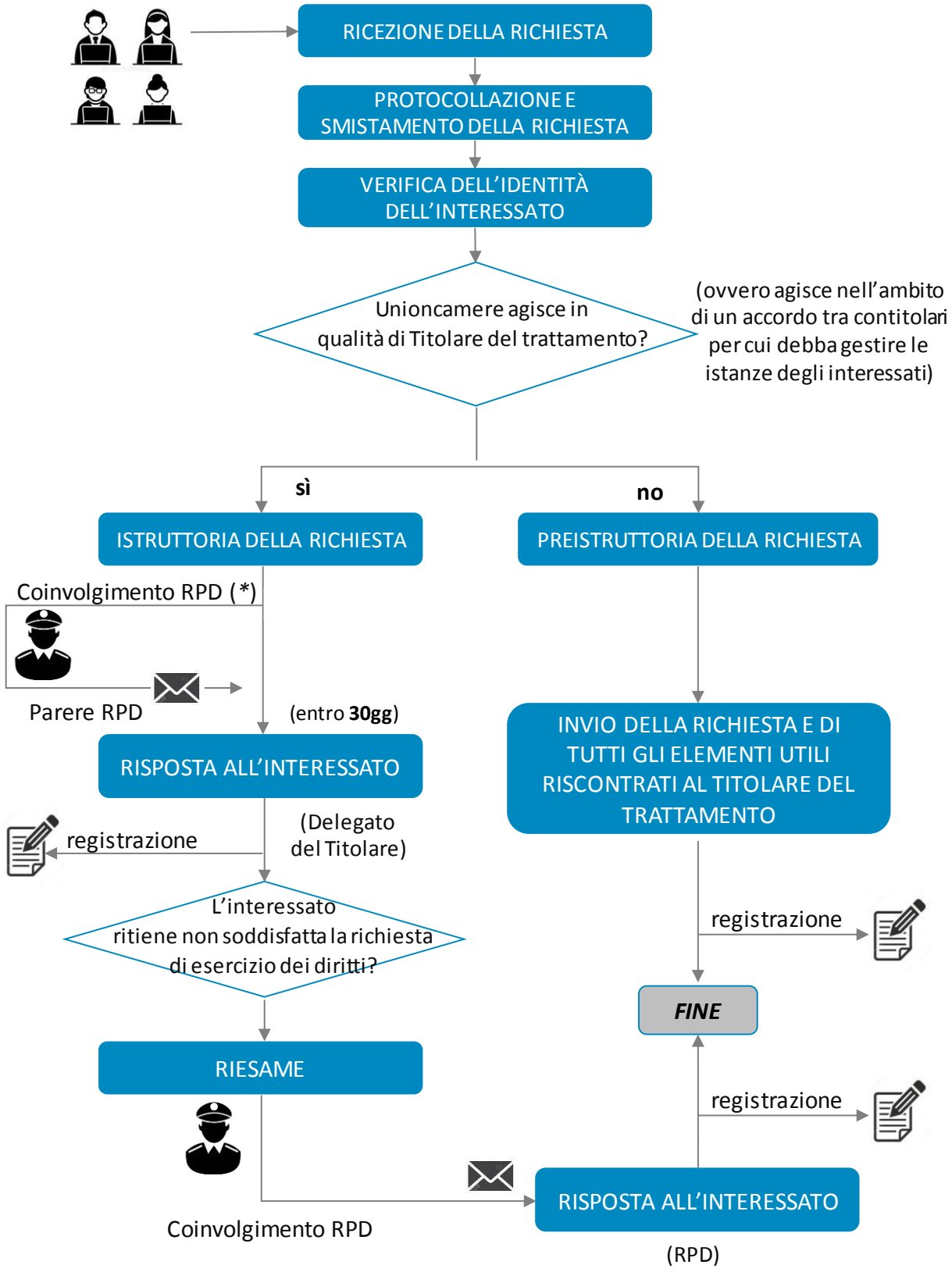
- Unioncamere dovrà gestire direttamente tutte le richieste di esercizio dei diritti che pervengano da interessati in relazione ai quali l'Ente assume la qualifica di Titolare del trattamento (anche se intercettate da soggetti terzi individuati ed operanti, ad es., in qualità di Responsabili del trattamento ex art. 28)
- in relazione a particolari trattamenti per i quali Unioncamere dovesse operare in qualità di Contitolare, è necessario verificare nell'atto convenzionale o nello specifico accordo stipulato con la/le controparti, ai sensi dell'art. 26 del GDPR, a chi competa gestire la procedura; se compete alla controparte, Unioncamere provvederà ad inoltrare la richiesta, assicurando comunque quanto riportato al par. seguente[2]
- in relazione ai trattamenti per i quali Unioncamere operi in qualità di responsabile esterno ai sensi dell'art. 28, l'Ente avrà l'onere esclusivamente di "*assistere il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato*" (art. 28, par. 3, lett. e del GDPR)

[1] Ai sensi dell'art. 4, n. 1), del GDPR per "interessato" si intende la persona fisica identificata o identificabile cui si riferiscono i dati personali. Sono interessati, quindi, sia i dati degli utenti finali dei servizi/Progetti di Unioncamere che persone fisiche con cui lo stesso ha rapporti diretti e di cui acquisisce e gestisce dati personali (es., componenti degli organi, dipendenti, professionisti, collaboratori di imprese appaltatrici…)

[2] Si specifica in proposito che il contenuto minimo dell'accordo/convenzione (ovvero la situazione di contitolarità, il titolare che si assume l'obbligo di evadere le richieste di esercizio dei diritti, il punto unico di contatto con l'interessato) dovrebbero essere elementi esposti nell'informativa ex art. 13 o 14 del GDPR, ferma restando la previsione di cui al par. 3 dell'art. 26 per cui "l'interessato… può esercitare i propri diritti … nei confronti di e contro ciascun titolare del trattamento".

## FASI DEL PROCESSO

Il flusso di gestione di una richiesta di esercizio dei diritti è di seguito rappresentato:




(*) nel caso in cui la richiesta pervenga al RPD, questi coinvolgerà, previa istruttoria, il delegato del titolare competente.

## RICEZIONE ED ISTRUTTORIA DI UNA RICHIESTA DI ESERCIZIO DEI DIRITTI

La richiesta può pervenire ad Unioncamere ad es., attraverso i dati di contatto presenti nelle varie informative rilasciate, direttamente al RPD[3] (nel qual caso questi può dare supporto ed orientamento al delegato del Titolare competente) ovvero essere intercettata da soggetti terzi che - operando in qualità di Responsabili esterni - si trovino in contatto diretto con gli interessati stessi per conto di Unioncamere. Per gestire correttamente quest'ultima eventualità, è necessario che tutti i contratti o atti giuridici analoghi (ad es., lettere di nomina) a responsabili esterni prevedano[4] l'obbligo di:

a) informare immediatamente Unioncamere di qualsivoglia richiesta di esercizio dei diritti ricevuta direttamente in relazione a trattamenti di cui Unioncamere sia titolare, anche se gestita spontaneamente dal responsabile esterno;
b) fornire i dati, le informazioni e tutta la collaborazione necessaria affinché la stessa Unioncamere possa assolvere al dovere di risposta nei confronti dell'interessato (ex art. 28, par. 3, lett. e), del GDPR).

Le richieste possono essere esercitate senza particolari formalità (a mezzo posta, anche elettronica, o fax), anche oralmente se ciò sia sufficiente, preferibilmente utilizzando l'apposito format di "esercizio dei diritti" di cui all'All. 2, pubblicato sia nella sezione "privacy"[5] che nella sezione "Trattamento dati personali e Responsabile della protezione dei dati"[6] del sito istituzionale. Il citato format è conforme a quello aggiornato dal Garante ai sensi del GDPR.

Con riferimento alle richieste pervenute oralmente (ad es., telefonicamente), è opportuno che il referente Unioncamere che riceve la richiesta provveda a tracciare gli elementi informativi necessari (compresi i dati necessari per contattare in caso di necessità l'interessato nel corso dell'istruttoria), richiedendo la compilazione all'interessato, ovvero provvedendo a compilare autonomamente il format precedentemente indicato. Può essere chiesto all'interessato di inviare una apposita mail alla casella dell'RPD.

Ove pervenute ai contatti istituzionali di Unioncamere esposti nell'informativa, la richiesta è gestita:

- dall'Ufficio Protocollo, ove pervenuta in modalità digitale:
- dalla Segreteria Generale e di Presidenza, ove pervenuta in forma cartacea.

In entrambi i casi il ricevente deve:

a) sottoporre a **protocollazione** la richiesta, al fine di attribuirvi la data di ricezione utile al calcolo dei termini di cui al par. successivo,
b) provvedere a **smistare** la richiesta al "delegato del Titolare"[7] ritenuto competente *ratione materiae*, ove desumibile dalla richiesta.

La competenza sulla gestione di una richiesta spetta, in linea di principio, all'Area/Ufficio che detiene i dati o i documenti oggetto di trattamento, secondo quanto riportato all'interno del Registro dei trattamenti di Unioncamere (competenza *ratione materiae*); in caso di dubbio sulla competenza, il soggetto che deve effettuare lo smistamento può fare riferimento alla segreteria generale per identificare nel modo migliore il destinatario della richiesta.

In caso di assenza di indicazioni che possano guidare tale fase la segreteria generale deve contattare l'interessato al fine di acquisire elementi utili a comprendere il contesto della richiesta.

Requisito soggettivo per l'esercizio dei diritti di cui trattasi è che le richieste si riferiscano ad informazioni relative a "**persone fisiche**" (in quanto le persone giuridiche sono escluse dal campo di applicazione della normativa) detenuti da Unioncamere o che si presume lo siano. L'interessato che esercita un diritto deve essere correttamente **identificato,** ai fini della più corretta istruttoria delle richieste, della successiva eventuale trasmissione dei dati e documenti o della valutazione su come trattare una pluralità di domande identiche (seriali) o onerose (vessatorie) da parte di uno stesso soggetto. Alla richiesta formulata nelle varie modalità precedentemente indicate dovrà dunque essere allegata – a pena di irricevibilità[8] - copia del documento d'identità del richiedente; in caso di assenza, il delegato del Titolare che gestisce l'istanza dovrà attivarsi tempestivamente con l'interessato per perfezionare la stessa.

Nel merito, l'istruttoria della richiesta può essere evasa dal referente interno all'Area responsabile dell'attività/progetto, con l'eventuale coinvolgimento del RPD, provvedendo quindi alla raccolta di tutti gli elementi utili al fine di fornire un idoneo riscontro alle richieste formulate.

---

[3] Art. 38, par. 4 GDPR: "Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento".
[4] secondo il format di cui alle Linee guida per l'allocazione delle responsabilità a soggetti esterni di Unioncamere.
[5] http://www.unioncamere.gov.it/P42A0C671S75/Privacy.htm
[6] http://www.unioncamere.gov.it/P42A3726C1937S1919/trattamento-dati-personali-e-responsabile-protezione-dei-dati.htm
[7] cfr. in proposito il Modello organizzativo, ruoli e sistema di responsabilità di Unioncamere.
[8] Si pensi alla circostanza per cui un soggetto richieda dati ed informazioni relativi ad altra persona fisica (interessato) simulando di essere l'interessato di cui esercita i diritti.

## RISCONTRO AGLI INTERESSATI

SCENARIO 1: Unioncamere, in qualità di **Titolare del trattamento**, deve fornire un idoneo riscontro all'interessato al più tardi entro 30 giorni dal ricevimento della richiesta, prorogando eventualmente tale termine ove necessario per ulteriori 60 giorni[9] ma sempre informando l'interessato di tale circostanza entro i primi 30 giorni (art. 12, par. 3 GDPR). Ove la richiesta non consenta di fornire un idoneo riscontro per mancanza di elementi sostanziali, il delegato che gestisce l'istruttoria può richiedere all'interessato di specificare ulteriori elementi informativi.

Unioncamere deve operare comunque agevolando il più possibile l'esercizio dei diritti da parte degli interessati, semplificandone le modalità e riducendo i tempi per la risposta.

La risposta deve essere formalizzata assecondando, per quanto possibile, le eventuali modalità richieste specificamente dall'interessato, e quindi:

- sempre "in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro";
- per iscritto o con altri mezzi, anche oralmente se così richiesto; in questo caso è fondamentale, anche ai fini del principio di accountability, far seguire sempre una risposta per iscritto (ad es., email) ovvero procedere al tracciamento/documentazione (nelle forme ritenute più opportune, ad es. mediante processo verbale) dell'assolvimento della richiesta;
- con mezzi elettronici, se l'interessato presenta la richiesta mediante mezzi elettronici, salvo diversa indicazione dell'interessato stesso.

Il riscontro può dare i seguenti esiti:

a) **accoglimento** della richiesta, nelle forme e modalità previste dai singoli diritti e dall'interessato;
b) **diniego** all'esercizio dei diritti, ad esempio nei seguenti casi generali o specifici:
   - difetto di legittimazione soggettiva (ad es., la richiesta riguarda dati riferiti a terzi o a persone giuridiche);
   - richiesta rientrante in uno degli ambiti di limitazione generale di cui al par. seguente, ove ne ricorrano i presupposti di legge;
   - siano ritenute prevalenti le finalità o basi giuridiche vantate dal Titolare nei casi specificamente previsti (ad es., obblighi di legge, di contratto, interesse pubblico prevalente, etc.), ovvero non siano valutate positivamente le specifiche "condizioni" per l'esercizio vantate dal richiedente[10].

SCENARIO 2: nel caso in cui la richiesta sia relativa ad un trattamento per il quale **Unioncamere assume il ruolo di Responsabile esterno del trattamento** (ovvero nei casi di **contitolarità** ove sia previsto che i rapporti con gli interessati siano gestiti da altro titolare), il delegato del Titolare cui la richiesta fa riferimento:

- provvede ad una pre-istruttoria preliminare, al fine di rilevare gli elementi informativi da contestualizzare al Titolare;
- provvede ad informare il Titolare della richiesta e della pre-istruttoria effettuata, garantendogli tutto il supporto possibile nell'evasione della stessa.

Il delegato del Titolare provvede quadrimestralmente a formalizzare un report al RPD contenente tutte le informazioni di cui all'All. 3 "Registro delle richieste di esercizio dei diritti degli interessati".

Il RPD provvede a registrare le informazioni rilevanti e ad alimentare lo specifico KPI di cui al par. "Indicatori di anomalia del sistema privacy" del documento Modello organizzativo, ruoli e sistema di responsabilità di Unioncamere.

## ULTERIORI INFORMAZIONI

L'esercizio di un diritto è di regola gratuito, tranne nel caso in cui

a) il titolare debba sostenere delle spese tecniche rilevanti per adempiere (es., qualora siano state richieste più copie);
b) le richieste risultino manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo (es. vessatorie).

in questi casi è possibile:

- addebitare un contributo spese (sub a e b), tenendo conto dei costi amministrativi sostenuti;
- rifiutare di soddisfare la richiesta (se sub b).

All'interessato che non ritenga soddisfatto l'esercizio dei propri diritti deve essere sempre assicurata la possibilità di adire direttamente il RPD di Unioncamere, indicando tale possibilità (ed i dati di contatto del RPD) all'interno della risposta formalizzata.

Naturalmente l'interessato potrà sempre proporre:

[9] se le operazioni necessarie per un integrale riscontro sono di particolare complessità, ovvero ricorre altro giustificato motivo
[10] per le limitazioni previste in relazione all'esercizio di ogni singolo diritto, che possono quindi comportare un diniego alla richiesta, si faccia riferimento più diffusamente all'All. 1.

- reclamo all'Autorità Garante per la protezione dei dati personali;
- ricorso giurisdizionale.

## LIMITAZIONI GENERALI AI DIRITTI ESERCITABILI

Oltre a limitazioni specificamente previste dal GDPR per l'esercizio di ogni singolo diritto (cfr. All. 1), sono ammesse **deroghe generali tematiche all'esercizio dei diritti** riconosciuti dal regolamento, sul fondamento di disposizioni normative nazionali, nei seguenti ambiti:

a) sicurezza nazionale, difesa o sicurezza pubblica;
b) prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;
c) **altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario**, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;
d) salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;
e) attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;
f) funzioni di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);
g) tutela dell'interessato o dei diritti e delle libertà altrui;
h) esecuzione delle azioni civili.

Il considerando 73 include inoltre espressamente, tra i possibili ambiti di limitazione, "**la tenuta di registri pubblici per ragioni di interesse pubblico generale**".
E' comunque da specificare che l'ambito di limitazione deve essere esattamente identificato dalle disposizioni, così come le numerose ulteriori informazioni di cui all'art. 23, par. 2, per cui tali – in assenza di interventi normativi – la compressione dei diritti è percorribile solo ove le disposizioni attualmente vigenti specifichino:

- le finalità del trattamento o le categorie di trattamento e le categorie di dati personali;
- la portata delle limitazioni introdotte;
- le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti;
- l'indicazione precisa del titolare del trattamento o delle categorie di titolari;
- i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento;
- i rischi per i diritti e le libertà degli interessati; e
- il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

## MATRICE DELLE RESPONSABILITA'

**Legenda**

- R = Responsabile
- C = Coinvolto
- I = Informato

| *Fase* | *Attività* | Dirigente delegato del Titolare | Segreteria Generale e di Presidenza | Ufficio protocollo | Responsabile della Protezione dei Dati | Società esterne Responsabili del trattamento | | |
|---|---|---|---|---|---|---|---|---|
| | *Soggetto/ Struttura* | | | | | | | |
| ***RICEZIONE ED ISTRUTTORIA*** | Ricezione della richiesta | | R | R | | | | |
| | Protocollazione della richiesta e smistamento | | R | R | | | | |
| | Verifica dell'identità dell'interessato | | R | R | | | | |
| | | | | | | | | |
| ***RISCONTRO*** | Raccolta informazioni | R | | | C | C | | |
| | Evasione della richiesta | R | | | I | C | | |
| | Formalizzazione esito | R | | | I | | | |
| | | | | | | | | |
| ***RIESAME*** | Ricezione della richiesta | | | | R | | | |
| | Riesame della richiesta | C | | | R | C | | |
| | Formalizzazione esito | I | | | R | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

## ALLEGATO 1 – FAQ DIRITTI DEGLI INTERESSATI

### Diritto di accesso dell'interessato (art. 15)

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere **l'accesso ai dati personali** e alle seguenti informazioni:

- le finalità del trattamento;
- le categorie dei dati personali di cui il titolare è in possesso;
- i destinatari cui i dati sono stati o saranno comunicati, specificando in particolare se si tratta di soggetti che si trovano in paesi terzi rispetto all'Unione Europea o se si tratta di organizzazioni internazionali. In particolare, qualora ricorra una di queste ultime ipotesi, l'interessato ha anche il diritto di essere informato sull'esistenza di adeguate garanzie concernenti il trasferimento dei suoi dati personali come precisato nel Capo V del GDPR, dedicato proprio ai trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali;
- se possibile, la durata prestabilita del periodo di conservazione dei dati o quanto meno i criteri cui il titolare fa riferimento per determinare tale durata;
- l'esistenza del suo diritto:
  - ✓ a chiedere la rettifica o la cancellazione dei dati;
  - ✓ a chiedere la limitazione del trattamento dei dati personali;
  - ✓ di opporsi al loro trattamento, perché ritenuto illegittimo;
- il diritto di proporre un reclamo al Garante per la protezione dei dati personali quando ritiene che vi sia stata violazione dei propri diritti o delle proprie libertà;
- tutte le informazioni disponibili sull'origine dei dati nel caso in cui non siano stati raccolti presso l'interessato, ma ricevuti da soggetti terzi (ai quali l'interessato potrebbe aver dato il consenso anche a tal fine) oppure ottenuti tramite elenchi pubblici;
- infine, la logica su cui è basato un **processo automatizzato**, come ad esempio la profilazione, e il funzionamento di tali meccanismi e le possibili conseguenze del loro utilizzo (ovvero in cosa consistono sostanzialmente, quali dati e come vengono elaborati).

Si tratta di un diritto assoluto, non soggetto a motivazione da parte dell'interessato né ad alcuna limitazione specifica, ad esclusione di quelle generali di cui all'art. 23 del GDPR.

Ove si tratti una notevole quantità d'informazioni riguardanti l'interessato, il titolare dovrebbe poter richiedere che l'interessato precisi, prima che siano fornite le informazioni, a quali dati o attività di trattamento la richiesta si riferisca.

Il diritto d'accesso può essere esercitato anche più volte e con una cadenza periodica, perché solo mediante un controllo costante l'interessato sarà davvero consapevole delle attività che riguardano i propri dati personali, sempre che le richieste non assumano un carattere vessatorio (pluralità di domande identiche, seriali o onerose da parte di uno stesso soggetto).

Il Titolare è tenuto ad adottare tutte le misure ritenute adeguate, prime tra tutte quelle atte a verificare l'identità di chi chiede l'accesso, con particolare attenzione ai casi in cui ciò avvenga direttamente online. Inoltre, l'esercizio del diritto in esame non dovrebbe pregiudicare i diritti e le libertà degli altri interessati. Il Considerando n. 63, al riguardo, fa riferimento ai segreti industriali e ai diritti di proprietà industriale (si pensi alla tutela dei diritti d'autore relativi a software).

### Diritto di rettifica (art. 16)

Tale diritto è esercitabile dall'interessato ove vi sia la necessità di **correggere**, **modificare** od **integrare** i dati poiché **errati, non aggiornati** o **insufficienti.** La correzione dei dati da parte del titolare deve avvenire senza ingiustificato ritardo.
Per la propria natura, si ritiene che il diritto possa essere esercitato solo su dati elementari, ma non in riferimento ad informazioni di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo.
È opportuno che anche per l'esercizio di questo diritto siano predisposti strumenti e sistemi in grado di facilitare l'accesso diretto dell'interessato alle informazioni che lo riguardano, così da permettergli di intervenire prontamente e, per quanto possibile, autonomamente per modificare i dati inesatti.

Nel caso in cui i dati personali oggetto di rettifica siano stati **comunicati** ad altri soggetti (o **pubblicati**), è onere del titolare darne comunicazione e richiedere la rettifica a ciascuno dei destinatari, a meno che ciò sia impossibile o implichi uno sforzo sproporzionato (art. 19 del GDPR).

## Diritto alla cancellazione (c.d. "diritto all'oblio" - art. 17)

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo nei seguenti casi:

a) i dati personali **non sono più necessari** rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato **revoca il consenso** su cui si basa il trattamento (rilasciato a sensi dell'art. 6, par. 1., lett. a), o dell'art. 9, par. 2, lett. a), se non esiste nessun'altra base giuridica che lo legittimi (in questo caso particolare assume rilevanza l'acquisizione del consenso da un minore, considerato non pienamente consapevole dei rischi derivanti dal trattamento: vedasi art. 8, parr. 1 e 2).
c) l'interessato si **oppone al trattamento** e non sussiste alcun ulteriore motivo legittimo per procedere al trattamento, oppure si oppone al trattamento dei propri dati per finalità di marketing diretto (compresa la profilazione nella misura in cui sia connessa a tale marketing diretto); in questo caso quindi la cancellazione è diritto susseguente a quello di cui all'art. 21
d) i dati personali sono stati trattati **illecitamente**;
e) i dati personali **devono essere cancellati per adempiere un obbligo legale** previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento
f) i dati personali sono stati raccolti relativamente **all'offerta di servizi della società dell'informazione ai minori**.

Il titolare del trattamento nei casi indicati è obbligato a procedere alla cancellazione dei dati e – se li ha resi pubblici - ad adottare le misure ragionevoli per informare altri titolari del trattamento che stanno trattando i dati (compreso "qualsiasi link, copia o riproduzione") di procedere alla loro cancellazione (art. 19 del GDPR).

Il diritto in argomento trova naturalmente alcune limitazioni che si fondano sulla base giuridica a fondamento del trattamento e che legittimano quindi sia la conservazione dei dati che l'ulteriore trattamento; il Titolare può quindi rigettare la richiesta di cancellazione se il trattamento si basa:

- sull'esercizio del diritto alla libertà di espressione e di informazione;
- su un adempimento di un obbligo legale, per l'esecuzione di un compito di pubblico interesse oppure nell'esercizio di pubblici poteri;
- su motivi di interesse pubblico nel settore della sanità pubblica;
- su finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui la cancellazione rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
- sull'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

## Diritto di limitazione del trattamento (art. 18)

Si tratta di una **sospensione** temporanea (ma che può anche diventare permanente) del trattamento in corso.
Il diritto è esercitabile ove ricorra almeno una delle seguenti ipotesi:

1) l'interessato ha contestato l'esattezza dei dati personali, in attesa della eventuale rettifica degli stessi;
2) il trattamento è illecito e l'interessato non richieda o si opponga alla cancellazione dei dati personali;
3) i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, mentre al titolare del trattamento non servono più ai fini del trattamento;
4) l'interessato si è opposto al trattamento (ai sensi dell'art. 21 del GDPR) e si è in attesa delle verifiche necessarie per determinare se i motivi legittimi del titolare del trattamento prevalgano su quelli dell'interessato.

I dati il cui trattamento sia sottoposto a limitazione **possono essere conservati ma non più trattati negli ambiti per cui sia stata accordata la limitazione, a meno che:**

a) il titolare non ottenga contestualmente uno specifico consenso per una o più finalità diverse da quelle per cui sia disposta la sospensione (ove il trattamento si basi sul consenso);
b) il trattamento non sia:
   - ✓ finalizzato all'esercizio o difesa di un diritto in sede giudiziaria;
   - ✓ finalizzato alla tutela dei diritti di un'altra persona fisica o giuridica;
   - ✓ effettuato per motivi di interesse pubblico rilevante.

Nel caso in cui i dati personali oggetto di limitazione siano stati **comunicati** ad altri soggetti (o **pubblicati**) e sia accordata la limitazione, è onere del titolare darne comunicazione a ciascuno dei destinatari, a meno che ciò sia impossibile o implichi uno sforzo sproporzionato (art. 19 del GDPR).
In un secondo momento la limitazione può essere revocata (ad es., a seguito dell'avvenuta rettifica); prima che la revoca sia efficace però, il titolare del trattamento deve avvisare l'interessato.

Il Considerando 67 illustra alcune modalità pratiche per attuare il diritto alla limitazione; questo potrebbe essere garantito ad es.:

- trasferendo temporaneamente i dati selezionati in un altro sistema di trattamento (così da non renderli disponibili per le normali attività di trattamento);
- rendendo i dati personali selezionati inaccessibili agli utenti (ove il trattamento sia così configurato);
- rimuovendo temporaneamente i dati pubblicati da un sito web.

Lo stesso considerando, poi, evidenzia che "negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe, in linea di massima, essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati (ove l'interessato non ne richieda la cancellazione). Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato". In questo senso, **il dato personale soggetto a limitazione dovrebbe essere "contrassegnato"** in attesa di determinazioni ulteriori.

## Diritto alla portabilità dei dati (art. 20)

Il diritto alla portabilità consente all'interessato di ricevere i dati personali forniti a un titolare, in un **formato strutturato**, **di uso comune** e **leggibile da dispositivo automatico**, e di trasmetterli a un altro titolare.

Non si applica ai trattamenti **non automatizzati** (quindi ad es., ai dati detenuti in archivi o registri cartacei) ed è esercitabile solo nel caso in cui i dati:

- ✓ siano stati **forniti direttamente dall'interessato** (consapevolmente e in modo attivo);
- ✓ siano acquisiti e trattati sulla base del **consenso** dell'interessato o per **l'esecuzione di un contratto** di cui è parte l'interessato (artt. 6, par. 1, lett. a), o 9, par. 2, lett. a)[11];
- ✓ siano **chiaramente riferibili all'interessato**[12]; sono quindi ad esempio esclusi i dati relativi a terze persone ovvero quelli anonimi;
- ✓ siano trattati attraverso **strumenti automatizzati**, ossia ad esclusione di qualsivoglia dato inferenziale o derivati, sia sulla base di un intervento umano nel trattamento medesimo[13] sia che ciò derivi ad es., dall'applicazione di un algoritmo[14];

L'interessato può quindi richiedere:

- di **ricevere i dati personali** trattati e conservarli su un supporto personale in vista di un utilizzo ulteriore per scopi personali, senza trasmetterli necessariamente a un altro titolare;
- di **trasmettere i dati personali** da un titolare del trattamento a un altro titolare del trattamento, se è tecnicamente fattibile.

Il titolare del trattamento può consentire di esercitare il diritto o fornendo uno strumento per il download dei dati, o garantendo la trasmissione diretta dei dati ad altro Titolare (anche il titolare ricevente i dati è soggetto a specifici obblighi, in particolare diventa il nuovo titolare e quindi deve garantire che i dati non siano eccessivi rispetto al servizio che fornisce).

Tenuto conto della molteplicità di categorie di dati potenzialmente oggetto di trattamento, la scelta del formato di rilascio dei dati più idoneo dipenderà dallo specifico settore di attività: si possono utilizzare formati di impiego comune, se già esistenti, oppure utilizzare formati aperti (es. XML), ovvero sviluppare formati interoperabili (cioè un formato che ne consenta il riutilizzo) e strumenti informatici che consentano di estrarre i dati pertinenti; in ogni caso, la scelta dello specifico formato deve essere ispirata all'obiettivo ultimo dell'interoperabilità. Ciò, tuttavia, non significa che i titolari debbano dotarsi di sistemi compatibili. Inoltre, i titolari dovrebbero fornire, unitamente ai dati, quanti più metadati

[11] Quindi ad es., non è esercitabile ove il trattamento si fondi su un obbligo di legge, sull'interesse pubblico o sull´interesse legittimo del titolare.

[12] Il Gruppo di lavoro WP 29 raccomanda ai titolari del trattamento di non interpretare l'espressione "dati personali che riguardano l'interessato" in modo eccessivamente restrittivo, qualora vi siano dati personali di terzi all'interno di un insieme di dati che riguardano l'interessato e sono stati forniti da quest'ultimo, e che l'interessato utilizza per scopi personali. Si può ritenere che un dato personale sia fornito dall'interessato se quest'ultimo lo "fornisce" consapevolmente e in modo attivo (per esempio, dei dati di registrazione - indirizzo postale, nome utente, età, ecc. - inseriti compilando un modulo online). Tuttavia, la definizione comprende anche i dati generati e raccolti attraverso le attività dell'utente che fruisce di un servizio o utilizza un dispositivo (es.: la cronologia delle ricerche effettuate dall'interessato, i dati relativi al traffico, i dati relativi all'ubicazione). Viceversa, il diritto alla portabilità non si applica ai dati personali che sono derivati o dedotti dalle informazioni fornite dall'interessato (per esempio, il profilo-utente creato analizzando i dati grezzi di un contatore intelligente), poiché non si tratta di dati forniti dall'interessato bensì creati dal titolare del trattamento.

[13] Nel caso in cui dei dati personali vengono trattati all'inizio con strumenti automatizzati – si pensi ad esempio al caricamento di un cv su un sito specializzato nell'intermediazione di offerta e domanda di lavoro – e successivamente arricchiti attraverso l'intervento umano – ad esempio tramite il lavoro di un professionista delle risorse umane che crea una scheda profilata del candidato - si esclude solamente la portabilità di quei dati "derivati" dai dati originariamente forniti dall'interessato e ne caso concreto, il cv sarebbe ovviamente portabile, mentre la scheda arricchita dal professionista no.

[14] Ad es., l'esito di una valutazione concernente un profilo creato a fini di profilazione, l'attribuzione di uno score creditizio o altra valutazione di affidabilità (ad es., in relazione alla normativa antiriciclaggio in ambito bancario, etc.)

possibile al miglior livello possibile di granularità, così da preservare la semantica specifica delle informazioni oggetto di scambio.

L'esercizio del diritto alla portabilità non deve né ledere i diritti e le libertà altrui né pregiudicare nessuno degli altri diritti dell'interessato, che può, per esempio: continuare a fruire del servizio offerto dal titolare anche dopo un'operazione di portabilità; esercitare il diritto di cancellazione o di limitazione del trattamento.

### Diritto di opposizione (art. 21)

Tale diritto è esercitabile ove il trattamento:

a) si fondi sull'esecuzione di un compito di **interesse pubblico** o connesso all'esercizio di **pubblici poteri** (in ambito pubblico);

b) sia posto in essere nell'esercizio di un **legittimo interesse** del titolare del trattamento o di terzi (in ambito privato[15]);

c) sia effettuato a fini di **ricerca scientifica o storica o a fini statistici** a norma dell'articolo 89, par. 1 del GDPR, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

In questi casi, l'interessato può opporsi in qualsiasi momento, per motivi connessi alla **sua situazione particolare**, e quindi **motivando la sua richiesta**. Spetta dunque al Titolare l'onere di dimostrare che la base giuridica su cui si fonda il trattamento (compresa la necessità di accertamento, esercizio o difesa di un proprio diritto in sede giudiziaria) prevalgano sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato; ove accordi l'esercizio del diritto, il Titolare deve astenersi dal trattare ulteriormente i dati, anche se può comunque conservarli; in caso contrario, l'interessato deve comunque essere informato della possibilità di esercitare reclamo davanti al Garante per la protezione dei dati personali.

d) è finalizzato ad **attività di marketing diretto** (compresa la profilazione connessa al marketing diretto).

In questo caso, l'interessato può opporsi in qualsiasi momento. Si tratta quindi di un **diritto assoluto**, poiché non soggetto a motivazione e ad alcuna valutazione da parte del titolare. Anche in questo caso, se l'interessato esercita tale diritto, il Titolare deve esimersi dal procedere con il trattamento per finalità di marketing, potendo ben continuare eventuali diversi trattamenti che fondino il proprio presupposto su diverse basi (ad es., obbligazione contrattuale, l'interesse legittimo del titolare stesso, finalità che devono comunque essere rese esplicite all'interessato).

Nel contesto dell'**utilizzo di servizi della società dell'informazione**[16] e fatta salva la direttiva 2002/58/CE (relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche), l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

### Processo decisionale relativo alle persone fisiche, compresa la profilazione (art. 22)

Il Regolamento europeo definisce la **profilazione** all'art. 4, n. 4), come: "*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi ad 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*".
Il WP 29 specifica che la profilazione è integrata allorquando concorrano le seguenti tre caratteristiche:

- il trattamento sia svolto in forma automatizzata;
- esso abbia ad oggetto dati personali;
- il suo obiettivo sia quello di valutare aspetti personali di una persona fisica.

Mediante la profilazione, infatti, si raccolgono informazioni su un individuo (o gruppo di individui), si analizzano le sue caratteristiche o modelli di comportamento e si inserisce il profilo individuale in una certa "categoria" o "segmento" per dar luogo ad ulteriori valutazioni o previsioni riguardanti, ad esempio, la sua capacità di eseguire un'attività, i suoi interessi o comportamento probabile.
Il **processo decisionale automatizzato** induce a prendere decisioni solo attraverso mezzi tecnologici, (ossia senza il coinvolgimento umano) e può basarsi su dati forniti direttamente dall'interessato (ad es. tramite form o un questionario), oppure su dati ricavati da programmi traccianti (ad es. la geolocalizzazione individuale fornita da un app) o dati derivanti da profili precedentemente creati (ad es. l'affidabilità finanziaria in ambito creditizio).

---

[15] In quanto, ai sensi dell'art. 6, par. 1 ultimo capoverso, la base giuridica del legittimo interesse "non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti"

[16] le attività economiche svolte on line nonché qualsiasi alto servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi (combinato disposto dell'art. 2, co. 1 lett. a del D.Lgs. 70/2003 e dell'art. 1, co. 1, lett. b della legge 317/1986

La decisione automatizzata e la profilazione a volte sono separate, altre volte no: infatti può succedere che una decisione automatizzata venga presa senza aver creato un profilo dell'individuo e, al contrario, una decisione automatizzata possa trasformarsi in profilazione a seconda del modo in cui i dati vengono utilizzati.

L'art. 22, par. 1, del GDPR, prevede che l'interessato abbia il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida con effetti analoghi. Per **decisione basata unicamente sul trattamento automatizzato** si deve intendere una decisione presa senza il coinvolgimento di un essere umano che possa influenzare ed eventualmente cambiare il risultato attraverso la sua autorità o competenza.
Perché sia riconosciuto il diritto dell'interessato è necessario che tale decisione "*produca effetti giuridici o incida in modo analogo significativamente sulla sua persona".* Il riferimento agli "**effetti giuridici**" riguarda l'impatto che una decisione automatizzata può produrre sulla sfera giuridica dell'individuo (ad es. penalizzando il diritto di associazione, di voto, di libertà negoziale, di libera circolazione, etc.) ovvero tutte le circostanze che "in modo analogo" possano potenzialmente e significativamente influenzare i comportamenti e le scelte degli individui interessati. Il Considerando 71 del GDPR cita, come esempi di decisioni automatizzate che possono incidere sui diritti e le libertà degli individui in maniera rilevante, il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani.

L'art. 22 al par. 2 prevede che il diritto non si applichi:
1. quando la decisione è necessaria per la **conclusione o l'esecuzione di un contratto** tra l'interessato e un titolare del trattamento; in questo caso, la *necessità* di utilizzare decisioni automatizzate per l'esecuzione o conclusione di un contratto deve essere interpretata in modo restrittivo, ossia che il titolare deve essere in grado di dimostrare che la profilazione è necessaria e non sono disponibili mezzi alternativi meno invasivi;
2. quando la decisione è **autorizzata dal diritto** dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; specifiche disposizioni di diritto comunitario o interno possono quindi, in casi specifici, autorizzare il ricorso ad un processo di decisione automatizzata (ad es., per il monitoraggio e la prevenzione delle frodi e dell'evasione fiscale o per garantire la sicurezza e l'affidabilità di un servizio fornito dal titolare).
3. quando la decisione si basa sul **consenso esplicito** dell'interessato; il consenso deve consistere in una dichiarazione espressa e non desunto da *facta concludentia.*

In ambito di decisioni basate unicamente su un trattamento automatizzato, il Regolamento introduce la necessità di fornire all'interessato maggiori informazioni sulle modalità di creazione ed utilizzo di questi processi. Infatti, l'art. 13, par. 2, lett. f) e l'art. 15, par. 1, lett. h), stabiliscono il diritto dell'interessato di conoscere l'esistenza del processo decisionale automatizzato e, in particolare, di ottenere informazioni significative sulla logica utilizzata (i criteri assunti per raggiungere la decisione, senza che con ciò si debba necessariamente fornire una spiegazione complessa degli algoritmi utilizzati) e sulle conseguenze previste di tale trattamento (attraverso esempi bisognerà fornire informazioni su come il processo automatizzato potrebbe influenzare in futuro la persona interessata).

Tenuto conto dei rischi rilevanti sui diritti e libertà dell'interessato per queste tipologie di trattamento, il Regolamento, da un lato obbliga il titolare ad attuare misure appropriate e "rafforzate" di tutela (importante sarà anche prevedere modalità che verificano con regolarità la correttezza dei processi per limitare errori di classificazione o valutazione con impatto negativo sui soggetti profilati), dall'altro lato, all'art. 22, par. 3 riconosce il potere all'interessato di ottenere l'*intervento umano* da parte del titolare, di esprimere la propria opinione e di contestare la decisione, nei casi in cui tale decisione sia prevista per contratto o consentita dall'interessato. L'Intervento umano deve essere "effettivo" ossia poter intervenire sul procedimento con autonome valutazioni.

Infine, un processo decisionale automatizzato che coinvolga categorie particolari da dati, di cui all'art. 9, par. 1, è consentito solo in presenza del consenso esplicito dell'interessato o per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri.

## ALLEGATO 2 – FORMAT ESERCIZIO DIRITTI DELL'INTERESSATO

| | |
|---|---|
| Il/La sottoscritto/a[17] | |
| Nato/a a | |
| Il | |
| Codice Fiscale | |
| Residente in | |
| Recapito (telefono/email…) | |
| Modalità di risposta | |

esercita con la presente richiesta i seguenti diritti di cui agli artt. 15-22 del Regolamento (UE) 679/2016, ed in particolare:

**Accesso ai dati personali**

*(art. 15 del Regolamento UE 679/2016)*

☐ chiede conferma che sia o meno in corso un trattamento di dati personali che lo riguardano

☐ in caso di conferma, chiede di ottenere l'accesso a tali dati, una copia degli stessi, e tutte le informazioni previste alle lettere da a) a h) dell'art. 15, paragrafo 1, del Regolamento (UE) 2016/679, e in particolare;

- ☐ le finalità del trattamento;
- ☐ le categorie di dati personali trattate;
- ☐ i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- ☐ il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- ☐ l'origine dei dati (ovvero il soggetto o la specifica fonte dalla quale essi sono stati acquisiti);
- ☐ l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

_____
_____
_____
_____

*(indicare qualsivoglia elemento utile ad identificare il trattamento cui si fa riferimento ai fini della più corretta e rapida gestione della richiesta)*

*(barrare solo le caselle che interessano)*

**Richiesta di intervento sui dati**

*(artt. 16-18 del Regolamento UE 679/2016)*

chiede di effettuare le seguenti operazioni:

☐ rettificazione e/o aggiornamento dei dati (art. 16 del Regolamento (UE) 2016/679)

☐ cancellazione dei dati (art. 17, paragrafo 1, del Regolamento (UE) 2016/679), per i seguenti motivi:

a) _____
b) _____
c) _____

☐ nei casi previsti all'art. 17, paragrafo 2, del Regolamento (UE) 2016/679, l'attestazione che il titolare ha informato altri titolari di trattamento della richiesta dell'interessato di cancellare link, copie o riproduzioni dei suoi dati personali;

☐ limitazione del trattamento (art. 18) per i seguenti motivi:

- ☐ contesta l'esattezza dei dati personali;
- ☐ il trattamento dei dati è illecito;
- ☐ i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- ☐ l'interessato si è opposto al trattamento dei dati ai sensi dell'art. 21, paragrafo 1, del Regolamento (UE) 2016/679.

La presente richiesta riguarda:

_____
_____
_____
_____

*(indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento)*

*(barrare solo le caselle che interessano)*

[17] Allegare copia di un documento di riconoscimento

**Portabilità dei dati**[18]

*(art. 20 del Regolamento UE 679/2016)*

Con riferimento a tutti i dati personali forniti al titolare, chiede di:

☐ ricevere tali dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico;

☐ trasmettere direttamente al seguente diverso titolare del trattamento _____
_____
*(specificare i riferimenti identificativi e di contatto del titolare: .....)*

☐ tutti i dati personali forniti al titolare;
☐ un sottoinsieme di tali dati, ovvero: _____
_____
_____

La presente richiesta riguarda:
_____
_____
_____
*(indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento)*

*(barrare solo le caselle che interessano)*

**Opposizione al trattamento**

*(art. 21, par. 1 del Regolamento UE 679/2016)*

☐ si oppone al trattamento dei suoi dati personali ai sensi dell'art. 6, paragrafo 1, lettera e) o lettera f), per i seguenti motivi legati alla sua situazione particolare:
_____
_____
_____
_____
_____

**Opposizione al trattamento per fini di marketing diretto**

*(art. 21, par. 2 del Regolamento UE 679/2016)*

☐ si oppone al trattamento dei dati effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale

Il sottoscritto:
☐ chiede di essere informato, ai sensi dell'art. 12, paragrafo 4 del Regolamento UE 679/2016, al più tardi entro un mese dal ricevimento della presente richiesta, degli eventuali motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste.

☐ chiede, in particolare, di essere informato della sussistenza di eventuali condizioni che impediscono al titolare di identificarlo come interessato, ai sensi dell'art. 11, paragrafo 2, del Regolamento UE 679/2016.

**Eventuali precisazioni**

_____
_____
_____
_____
_____

*(fornire eventuali spiegazioni utili o indicare eventuali documenti allegati)*

Luogo, data e firma

[18] Per approfondimenti: Linee-guida sul diritto alla "portabilità dei dati" - WP242, adottate dal Gruppo di lavoro Art. 29, disponibili in www.garanteprivacy.it/regolamentoue/portabilita.

## ALLEGATO 3 – REGISTRO RICHIESTE ESERCIZI DIRITTI INTERESSATI

| N. record/anno | Data arrivo della richiesta | Tipologia diritto/reclamo esercitato | Oggetto della richiesta | Trattamento di riferimento | Responsabile della risposta | Esito (diniego, accoglimento, accoglimento parziale) | Data invio risposta | Richiesta riesame RPD[19] (sì/no, data) | Esito riesame RPD e data |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

[19] Ove la risposta sia formalizzata da un Dirigente/Quadro di Unioncamere e l'interessato richieda il riesame della decisione assunta al RPD