**Allegato R)**

# Procedura “DPIA”

## “Data Protection Impact Assessment”

## Regolamento UE 679/2016

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | |
| 01 | 00 | 25.07.18 | Prima Emissione | RPD | RTPD | Titolare |
| **Edizione** | **Revisione** | **Data** | **Descrizione** | **Redatto** | **Verificato** | **Approvato** |

**SOMMARIO**

## 1. SCOPO

La presente procedura ha lo scopo di definire le modalità da seguire, ove richiesto, per una valutazione di impatto sulla protezione dei dati personali, definita “Data Protection Impact Assessment”, di seguito “DPIA”, e le relative responsabilità.

## 2. CAMPO DI APPLICAZIONE

La procedura è applicabile a tutte le attività svolte da Formez PA (di seguito il titolare del trattamento), con particolare riferimento alla gestione di tutti gli archivi/documenti cartacei e di tutti i sistemi informatici attraverso cui vengono trattati dati personali degli interessati (clienti, fornitori, altri soggetti terzi, ecc.), anche con il supporto di fornitori esterni.

## 3. DEFINIZIONI E ABBREVIAZIONI

### 3.1. Definizioni

Per l'elenco completo, si rimanda all'Art. 4 del REGOLAMENTO (UE) 2016/679

1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «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;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «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;

5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «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;

9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

15) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) «stabilimento principale»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo

stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «Autorità di controllo/Autorità»: l'autorità pubblica indipendente istituita da uno Stato membro; in Italia è il Garante per la protezione dei dati personali.

### 3.2. Abbreviazioni

**RPD** Responsabile per la protezione dei dati personali

**RTDP** Responsabile della tutela dei dati personali e della riservatezza dei dati aziendali

## 4. RESPONSABILITÀ

| | |
|---|---|
| RPD | • Attuazione della DPIA dal supporto alla valutazione dei rischi sino ai controlli e relative azioni adeguative, quando necessarie. |
| Responsabile di Area / Servizio | • Valutazione dei rischi ed attuazione delle azioni di correzione individuate. |
| RTDP | • Supervisione del processo |

## 5. MODALITÀ ESECUTIVE

### 5.1. Generalità

L’art. 35 del Regolamento, stabilisce che*: Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento,* ***una valutazione dell'impatto dei trattamenti*** *previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.*

Inoltre la norma prevede che: *La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:*

*a) 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;*

*b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o*

*c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.*

La Valutazione d’impatto o DPIA (Data Protection Impact Assessment) è una procedura finalizzata a descrivere un trattamento, valutare necessità e proporzionalità dello stesso, tenendo conto dei rischi per i diritti e le libertà delle persone fisiche derivanti da tale trattamento.

Attraverso la DPIA viene effettuata dal titolare la valutazione dei rischi e la definizione delle misure idonee ad affrontarli. La DPIA è uno strumento importante in termini di responsabilizzazione (accountability) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del Regolamento, ma anche a dimostrare l’adozione di misure idonee a garantire il rispetto di tali prescrizioni. La DPIA permette al Titolare di realizzare e dimostrare la conformità di uno specifico trattamento con le norme in materia di trattamento dei dati personali.

### 5.2. Necessità di effettuare la valutazione di impatto

Secondo le “Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento possa presentare un rischio elevato ai sensi del regolamento 2016/679” del WP29, adottate il 4 ottobre 2017, per definire la necessità di effettuare la valutazione di impatto è opportuno prendere in esame i seguenti nove criteri:

1. Valutazione o assegnazione di un punteggio, incluse la profilazione e la predizione, in particolare a partire da 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 (ad es. una banca che scremi i propri clienti tramite una banca dati di riferimento del credito, o una società di costruzione di profili comportamentali o di marketing in base all’utilizzo o alla navigazione sul suo sito web).
2. Decisioni automatiche con effetti giuridici o similmente significativi: elaborazione che mira a prendere decisioni su soggetti interessati e che produce effetti giuridici riguardanti la persona fisica o che allo stesso modo sia determinante per la persona fisica (ad es. il trattamento può comportare l’esclusione da determinati benefici).
3. Controllo sistematico: trattamento utilizzato per osservare, monitorare o controllare soggetti interessati, inclusi i dati raccolti attraverso un controllo sistematico di una zona accessibile al pubblico.
4. Trattamento di dati particolari: si tratta delle categorie particolari di dati ai sensi dell’articolo 9 del GDPR (dati personali che rivelino l'origine razziale o etnica, le

opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) oltre ai dati personali relativi a condanne penali o reati di cui all’art. 10.

5. Trattamenti di dati elaborati su larga scala: il GDPR non definisce cosa costituisca larga scala, anche se il considerando 91 fornisce alcune indicazioni. In ogni caso, il WP29 raccomanda che i seguenti fattori, in particolare, siano considerati per determinare se il trattamento è effettuato su larga scala:
    a. il numero di persone interessate, come numero specifico o come percentuale della popolazione di riferimento;
    b. il volume dei dati e / o la gamma di diversi elementi di dati in corso di elaborazione;
    c. la durata, o la permanenza, dell’attività di elaborazione dati;
    d. l’estensione geografica delle attività di elaborazione.
6. Combinazione o raffronto di insiemi di dati, ad esempio provenienti da due o più trattamenti effettuati per scopi diversi e / o da altri titolari in modo tale da superare le ragionevoli aspettative dell’interessato.
7. Trattamenti di dati relativi a interessati vulnerabili: il trattamento di questo tipo di dati può richiedere una DPIA a causa del maggiore squilibrio di potere tra interessato e titolare del trattamento, nel senso che il singolo può non essere in grado di acconsentire, o di opporsi, con facilità al trattamento dei propri dati, né può talora con facilità esercitare i propri diritti. La categoria degli interessati vulnerabili comprende anche i minori, i dipendenti, quei segmenti di popolazione particolarmente vulnerabile e meritevole di specifica tutela (soggetti con patologie psichiatriche, richiedenti asilo, anziani, pazienti) e ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento.

8. Utilizzi innovativi o applicazione di soluzioni tecnologiche o organizzative, come la combinazione fra l’uso di impronte digitali e il riconoscimento del volto per un migliore controllo di accesso fisico, ecc.
9. Trattamenti che impediscono agli interessati di esercitare un diritto o utilizzare un servizio o un contratto” (ad es. lo screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento).

Il WP29 ritiene che più sono i criteri inclusi nel trattamento, più è probabile che esso presenti un rischio elevato per i diritti e le libertà delle persone, e quindi richieda una DPIA. Come regola generale, un’operazione di elaborazione che includa meno di due criteri può non richiedere una DPIA per il minore livello di rischio, mentre operazioni di trattamento che soddisfino almeno due di questi criteri richiederanno una DPIA.

### 5.3. Metodologia

Il criterio utilizzato per l’analisi dei rischi, derivato con alcuni adattamenti dalla Norma DS/ISO/IEC 29134:2017 (Annex A) e dal documento “Privacy Impact Assessment” della Commission nationale de l’informatique et des libertés, 2015, si basa sulla correlazione fra la gravità (**G**) di un rischio (in relazione all’ampiezza degli impatti potenziali sugli interessati, tenendo conto delle misure esistenti) e la probabilità (**P**) di accadimento dell’evento che provoca il danno (in relazione alle vulnerabilità dei supporti interessati e alla capacità delle fonti di rischio di sfruttarle, tenendo conto delle misure esistenti).

A tal riguardo, si è definito l’indice di rischio **R** come funzione dell’Indice di probabilità per l’Indice di gravità del danno:

$$R = f(P, G)$$

e, conseguentemente, la priorità da assegnare alle misure da adottare per ridurre il rischio ad un livello ritenuto accettabile.

I riferimenti utilizzati per una oggettiva relazione fra livelli e valori di gravità e probabilità sono riportati di seguito.

*Gravità delle conseguenze per i diritti degli interessati (**G**) che il verificarsi dell'evento può produrre:*

- Livello **1** - **Trascurabile**: gli interessati non subiranno alcun impatto o potrebbero incontrare qualche inconveniente che supereranno senza difficoltà.
- Livello **2** - **Limitato**: gli interessati potrebbero sperimentare notevoli inconvenienti, che possono superare nonostante alcune difficoltà.
- Livello **3** - **Significativo**: gli interessati potrebbe avere conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative.
- Livello **4** - **Massimo**: gli interessati potrebbero avere conseguenze significative, anche irrimediabili, che potrebbero non essere superate.

*Probabilità o Frequenza (**P**) con cui potrebbe verificarsi un evento:*

- Livello **1** - **Trascurabile**: non sembra possibile che le minacce possano concretizzarsi.
- Livello **2** - **Limitato**: sembra difficile che le minacce possano concretizzarsi.
- Livello **3** - **Significativo**: sembra possibile che le minacce possano concretizzarsi.
- Livello **4** - **Massimo**: sembra molto facile che le minacce possano concretizzarsi.

I Livelli di Rischio associabili alle diverse possibilità che possono verificarsi incrociando i livelli definiti di Probabilità e Gravità, si possono raggruppare in 4 Classi di Priorità secondo lo schema seguente:

*Danno o Gravità (**G**)*

| | | | | |
|---|---|---|---|---|
| **4** | **Ma** | **Ma** | **E** | **E** |
| **3** | **Ma** | **Ma** | **E** | **E** |
| **2** | **B** | **B** | **Mb** | **Mb** |
| **1** | **B** | **B** | **Mb** | **Mb** |
| | **1** | **2** | | |

*Probabilità o Frequenza (**P***

- Priorità 1 - Livello di Rischio **Elevato**: questi rischi devono essere assolutamente evitati o ridotti applicando misure di sicurezza che ne riducano la gravità e la probabilità. Idealmente, dovrebbe anche essere garantito che vengano trattati contemporaneamente con misure di prevenzione (azioni prima del disastro), protezione (azioni durante il disastro) e recupero (azioni dopo il disastro).
- Priorità 2 - Livello di Rischio **Medio alto**: questi rischi devono essere evitati o ridotti applicando misure di sicurezza che ne riducano la gravità o la probabilità, favorendo le misure. Possono essere presi, ma solo se si dimostra che non è possibile ridurre la loro gravità e se la loro probabilità è trascurabile.
- Priorità 3 - Livello di Rischio **Medio basso**: questi rischi devono essere ridotti applicando misure di sicurezza che riducano la loro probabilità, favorendo le misure di recupero. Possono essere presi, ma solo se si dimostra che non è possibile ridurre la loro probabilità e se la loro gravità è trascurabile.
- Priorità 4 - Livello di Rischio **Basso**: è possibile prendere questi rischi, soprattutto perché il trattamento di altri rischi porta anche al loro trattamento.

### 5.4. Attuazione della DPIA

Nel Registro delle attività di trattamento dei dati di Formez PA è inclusa, e deve essere aggiornata a cadenza al minimo annuale, una sezione nella quale sono individuati i trattamenti effettuati dal titolare che richiedono un’analisi d’impatto.

In applicazione di tale determinazione sottoscritta dal Titolare, il RPD si attiva con le aree e/o servizi di Formez PA interessati per pianificare la specifica DPIA individuata come necessaria.

Il responsabile di Area o di Servizio, con il supporto del RPD, elabora la valutazione dei rischi e definisce in accordo con il RPD le misure di controllo, compilando il documento “DPIA e piano di trattamento dei rischi” in Allegato 1.

Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

Quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, il responsabile di Area o di Servizio, sentito il RPD, riesamina la valutazione dei rischi e le

misure di controllo e aggiorna l'Allegato 1.

## 6. RIFERIMENTI

- REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
- Decreto Legislativo 30 giugno 2003 n. 196, recante il Codice in materia di protezione dei dati personali e provvedimenti adottati dall’Autorità Garante per la protezione dei dati personali;
- Best practices di settore sviluppatesi alla luce del Codice e della giurisprudenza del Garante;
- Linee guida sulla notifica delle violazioni di dati personali ai sensi del Regolamento 679/2016 (WP250), adottate dal Gruppo di lavoro Articolo 29 (“WP29”), in via definitiva, il 6 febbraio 2018;
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento “possa presentare un rischio elevato” ai sensi del Regolamento 2016/679 (WP248), adottate dal WP29, in via definitiva, il 4 ottobre 2017;
- Linee guida sui responsabili della protezione dei dati (WP243), adottate dal WP29, in via definitiva, il 5 aprile 2017;
- Dichiarazione relativa al ruolo di un approccio basato sul rischio nel quadro normativo in materia di protezione dati (WP218), adottata dal WP29 il 30 maggio 2014;
- Raccomandazioni per una metodologia della valutazione della gravità delle violazioni di dati personali, adottate dalla European Union Agency for Network and Information Security (ENISA) il 20 dicembre 2013;
- ISO 27001 “Information technology – Information security management systems - Requirements”;

## 7. ARCHIVIAZIONE

I documenti allegati alla presente procedura sono archiviati da RPD.

## 8. ALLEGATI

Allegato 1 - Piano di trattamento dei rischi