Università
San Raffaele
Roma

MODELLO ORGANIZZATIVO PRIVACY (MOP) DI

UNIVERSITÀ TELEMATICA SAN RAFFAELE ROMA S.R.L.

AI SENSI DEL REGOLAMENTO EUROPEO 2016/679

Allegato 10.3 del Modello Organizzativo Privacy

Sistema delle Procedure Privacy (PP):
PP3 - Procedura per la compilazione della DPIA

Edizione n. 3

All. 10.3 – PP3: Procedura per la compilazione della DPIA

1. PREMESSA

Università Telematica San Raffaele Roma S.r.l. (di seguito anche *"Università"* o *"UTSR"*) ha adottato, e tiene costantemente aggiornato, un Modello Organizzativo Privacy (di seguito anche *"MOP"*) redatto ai sensi del Regolamento Europeo 2016/679.

Parte integrante del MOP è costituito dal Sistema delle Procedure Privacy (PP) che include la presente Policy.

2. SCOPO E APPLICABILITÀ

La presente Procedura vuole essere di supporto per una migliore gestione della Valutazione di impatto per i dati personali così come prevista dall'articolo 35 del Regolamento in materia di privacy 2016/679.

La DPIA (Data Protection Impact Assessment) è necessaria quando un certo trattamento, in ragione della sua natura, del suo oggetto e delle sue finalità, presenti un rischio elevato per i diritti e le libertà delle persone fisiche.

Ai sensi dell'articolo 35, c. 3 Reg. UE 16/679 una valutazione di impatto è necessaria quando il trattamento consiste in:

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 tra cui i dati sanitari e i dati relativi a condanne penali e a reati;
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

In ossequio al principio della c.d. *privacy by design*, per ogni nuovo progetto che possa coinvolgere trattamenti di dati comportanti i rischi menzionati, occorre interrogarsi sull'opportunità o meno di procedere con una valutazione di impatto.

I trattamenti per i quali effettuare la DPIA sono quelli già individuati nel Registro dei trattamenti.

3. PROCEDURA OPERATIVA E DOCUMENTAZIONE DI SUPPORTO

La metodologia per eseguire la Valutazione di impatto per i dati personali prevede l'elaborazione di n. 2 documenti:

1. **RELAZIONE SULLA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI:** consiste in un documento descrittivo l'analisi d'impatto sulla protezione dei dati suddiviso in una serie di sezioni contenenti le fasi di cui si compone la DPIA. Le sezioni della Relazione sono le seguenti:

    a) **ordine temporale degli aggiornamenti della DPIA**: consente di allocare le responsabilità e le co-responsabilità di redazione dell'analisi di impatto ivi incluse le eventuali condivisioni con le risorse esterne coinvolte al fine di acquisire taluni suggerimenti migliorativi;

b) Premessa normativa: è ritenuto utile prevedere, all'interno della Valutazione d'impatto, un preliminare richiamo ai contenuti dell'art. 35 Reg. UE 2016/679 che ha dato origine all'analisi anche al fine di ottemperare ad una completezza informativa nei confronti del lettore finale del documento;

c) informazioni generali e preliminari sul trattamento dei dati. Tale fase si compone dell'esplicitazione delle seguenti informazioni:

1. oggetto della DPIA: in questa sezione occorre inserire il nome, il suo acronimo e una sommaria descrizione indicandone lo scopo;
2. durata della DPIA: in questa sezione occorre indicare la data di decorrenza e la durata del trattamento dei dati oggetto di DPIA;
3. definizione dei criteri che hanno configurato la necessità della DPIA: si tratta di un elenco che il compilatore deve fleggare in corrispondenza del criterio applicabile all'analisi in oggetto. Tali criteri sono stati individuati dall'Autorità Garante per la Protezione dei Dati Personali e dal WP29;

d) informazioni specifiche sul trattamento dei dati. In ottemperanza all'art. 35, c. 7, lett. a) Reg. UE 2016/679 in questa sezione è riportata una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento.

Tale fase si compone dell'esplicitazione delle seguenti informazioni:

1.informazioni sulla struttura e allocazione delle responsabilità in termini di identificazione:

1.1 del Titolare del trattamento;

1.2 delle eventuali ulteriori figure coinvolte in qualità di Contitolari del trattamento ex art. 26 Reg. UE 2016/69;

1.3 del/dei Responsabile/i del trattamento ex art. 28 Reg. UE 2016/679;

2.informazioni sul trattamento dei dati in termini di identificazione:

2.1 delle categorie di dati trattati;
2.2 delle categorie Interessati;
2.3 delle risorse di supporto ai dati (supporti cartacei e supporti informatici);
2.4 del flusso di dati oggetto di trattamento dei dati;

e) analisi dei principi fondamentali: in ottemperanza all'art. 35, c. 7, lett. b) Reg. UE 2016/679 in tale sezione viene espressa una valutazione circa la necessità e la proporzionalità dei trattamenti in relazione alle finalità.

Nello specifico, si tratta dell'identificazione delle seguenti informazioni:

1. motivazioni che rendono gli scopi del trattamento specifici, espliciti e legittimi;

2. basi giuridiche che rendono lecito il trattamento dei dati (trattamento dei dati comuni, particolari e giudiziari);
3. motivazioni per le quali ogni dato raccolto è necessario per le finalità del trattamento;
4. misure previste per garantire la qualità dei dati;
5. termini di conservazione dei dati;
6. informazioni che saranno fornite agli Interessati e gli strumenti utilizzati per tale conferimento;
7. modalità di esercizio dei diritti dell'Interessato ai sensi degli artt. 15-21 Reg. UE 16/679;
8. modalità di ottenimento del consenso degli Interessati (ove applicabile);
9. ambito delle responsabilità di ogni Responsabile del trattamento ex art. 28 Reg. UE 2016/679 coinvolto e riferimenti ai contratti, ai codici di condotta e alle certificazioni ove sono fissati gli obblighi loro incombenti;
10. trasferimento dei dati al di fuori dell'Unione Europea;
11. trasferimento dei dati nei confronti di terzi;

f) **mappatura dei rischi:** si rinvia al dettaglio illustrato nel successivo punto n. 2;

g) **conclusioni:** tale sezione accoglie la dichiarazione del grado di rischio per i diritti e le libertà degli Interessati coinvolti nel trattamento tenuto conto delle finalità del trattamento e delle misure adottate nella gestione delle operazioni che hanno reso necessario una Valutazione d'impatto;

h) **riesame ed aggiornamento della DPIA:** la Relazione d'impatto dovrà essere riesaminata e aggiornata alla luce dei cambiamenti normativi e organizzativi relativi alla gestione delle operazioni di trattamento che hanno reso necessario la DPIA e in linea con i requisiti di protezione dei dati personali, al fine di revisionare periodicamente i mutamenti nei rischi legati al trattamento e le relative evoluzioni, anche a seguito delle risultanze emerse a fronte dell'esecuzione di eventuali Audit interni e/o esterni;

2. **MAPPATURA DEI RISCHI:** in ottemperanza all'art. 35, c. 7, lett. c) Reg. UE 2016/679 deve essere eseguita una mappatura dei rischi volta ad individuare eventuali e specifiche aree sensibili o selezionati processi a rischio di non conformità, parziale o totale.

Il livello di rischio residuo rappresenta un elemento determinante, ma di partenza, per la definizione delle eventuali ulteriori misure di controllo e/o correttive che devono essere adottate nelle fasi successive all'analisi dei rischi.

Il processo di valutazione del rischio parte dalla determinazione dell'impatto sull'Interessato (cioè sulla persona fisica a cui il dato riferisce) in caso di distruzione, perdita, modifica, divulgazione non autorizzata o altri avvenimenti negativi.

La tabella Excel allegata alla Relazione sulla Valutazione di impatto (allegato n. 1) illustra i rischi potenziali identificati e descrive il processo di analisi dei rischi come segue:

1.Aree di rischio rilevanti per la protezione dei dati: inserimento delle aree e dei processi a rischio in tema di trattamento dati personali.

2.Descrizione delle modalità di verificazione del rischio: inserimento delle modalità tramite le quali il rischio può verificarsi.

3.Impatto sui diritti e le libertà degli Interessati con descrizione del livello di rischio prima delle misure: inteso come il rischio che un'attività incorpora prima di considerare le misure di mitigazione del rischio messe in atto. È composto dalle seguenti voci:

- **PROBABILITÀ**: intesa come stima della probabilità di accadimento degli eventi sulla base della seguente scala di valutazione progressiva ➔ "MASSIMA", "ALTA", "MEDIA", "BASSA".
- **GRAVITÀ**: intese come stima della gravità dei danni attesi in relazione al verificarsi degli eventi sulla base della seguente scala di valutazione progressiva ➔ "MASSIMA", "ALTA", "MEDIA", "BASSA".
- **LIVELLO DI RISCHIO INIZIALE**: inteso come prodotto della probabilità e della gravità il cui risultato è misurabile in base alla seguente scala di valutazione progressiva ➔ "MASSIMA", "ALTA", "MEDIA", "BASSA".

4. Misure di mitigazione del rischio: elencazione delle misure a presidio del rischio inziale intese come misure/procedure tecniche ed organizzative attuate per prevenire e/o ridurre i rischi.

5. Livello di adeguatezza delle misure di mitigazione a fronte del rischio inziale: inteso come fattore che fornisce un'indicazione sull'adeguatezza delle misure di sicurezza implementate per ciascun rischio e viene illustrato, anche attraverso l'assegnazione di un valore numerico, come segue:

- **Adeguato**: misura di sicurezza efficace nel mitigare il rischio;
- **Parzialmente adeguato**: misura di sicurezza parzialmente efficace nel mitigare il rischio;
- **Inadeguato**: misura di sicurezza non efficace nel mitigare il rischio.

6. **Livello di rischio residuo**: inteso come il rischio non eliminato dalle misure di mitigazione del rischio in base al quale viene redatta la Valutazione finale e illustrato anche attraverso l'assegnazione di un valore che è il risultato della differenza tra il Livello di rischio *iniziale* e il Livello di adeguatezza. La scala progressiva di valutazione è la seguente:

- **Basso**: rischio gestibile che non incide significativamente sui diritti e le libertà degli Interessati;

- **Medio**: rischio parzialmente gestibile. Tuttavia, se non gestito adeguatamente tale rischio è in grado di determinare impatti significativi sugli Interessati (es. limitazioni dei diritti);
- **Alto**: rischio difficilmente gestibile e preoccupante per gli Interessati coinvolti che può determinare delle compressioni eccessive nell'esercizio dei diritti degli Interessati nonché scaturirne un trattamento illecito di dati personali;
- **Massimo**: rischio non gestibile con effetti gravosi o irreversibili per gli Interessati coinvolti.

7. **Ulteriori azioni di miglioramento:** intese come le suppletive misure da adottare al fine di mitigare ulteriormente il rischio.

Di seguito viene illustrata la versione standard del prospetto di mappatura dei rischi.

ALL. 1 DELLA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

NOME DEL PROGETTO: _____ DATA DI COMPILAZIONE: __/__/____

N.	Area di rischio	Descrizione delle modalità di verificazione del rischio	Impatto sui diritti e le libertà degli Interessati: descrizione del livello di rischio prima delle misure			Misure di mitigazione del rischio: illustrazione delle misure a presidio del livello di rischio iniziale		Livello di adeguatezza delle misure di mitigazione a fronte del rischio iniziale	Livello di rischio residuo *(Livello di rischio iniziale - livello di adeguatezza delle misure di sicurezza)*	Ulteriori azioni di miglioramento
			Probabilità	Gravità	Livello di rischio iniziale *(Probabilità x Gravità)*	Misure di sicurezza tecniche	Misure di sicurezza organizzative			
2										
3										
4										
5										
6										
7										
8										
9										
10										

Legenda dei valori di rischio:

- Massimo = rischi gravosi o irreversibili per gli Interessati coinvolti
- Alto = rischio preoccupante per gli Interessati coinvolti
- Medio = rischi di impatti significativi sugli Interessati
- Basso = rischi che non incidono significativamente sugli Interessati

Legenda del calcolo del rischio iniziale:

- Massimo x Massimo = Massimo
- Alto x Massimo = Massimo
- Medio x Massimo = Massimo
- Basso x Massimo = Alto
- Alto x Alto = Alto

- Alto x Medio = Alto
- Alto x Basso = Medio
- Medio x Medio = Medio
- Medio x Basso = Medio
- Basso x Basso = Basso

Legenda del livello di adeguatezza delle misure di mitigazione a fronte del rischio iniziale:

- 1 = Adeguato
- 2 = Parzialmente adeguato
- 3 = Inadeguato

Legenda del livello di rischio residuo:

- Massimo - Adeguato = Medio
- Massimo - Parzialmente adeguato = Alto
- Massimo - Inadeguato = Massimo
- Alto - Adeguato = Basso
- Alto - Parzialmente adeguato = Medio
- Alto - Inadeguato = Alto
- Medio - Adeguato = Basso
- Medio - Parzialmente adeguato = Basso
- Medio - Inadeguato = Medio
- Basso - Adeguato = Basso
- Basso - Parzialmente adeguato = Basso
- Basso - Inadeguato = Basso

Il presente documento è diffuso all'interno di Università Telematica San Raffaele Roma S.r.l. ed è comunicato ai destinatari del MOP che hanno l'obbligo di:

- conformarsi alle prescrizioni messe a punto dall'Università;
- astenersi dall'attuare comportamenti che possano, anche in modo potenziale o involontario, integrare una violazione nella gestione e nel trattamento dei dati.

La Direzione s'impegna a riesaminare periodicamente la **PP3 - Procedura per la compilazione della DPIA** affinché la gestione aziendale possa tendere ad un progressivo miglioramento delle prestazioni attuando le misure correttive ritenute necessarie.