REGIONE DEL VENETO
ULSS8 BERICA

Servizio Sanitario Nazionale - Regione Veneto
AZIENDA ULSS N. 8 BERICA
Viale F. Rodolfi n. 37 – 36100 VICENZA
COD. REGIONE 050–COD. U.L.SS.508 COD.FISC. E P.IVA 02441500242–Cod. iPA AUV
Tel. 0444 753111 - Fax 0444 753809 Mail protocollo@aulss8.veneto.it
PEC protocollo.centrale.aulss8@pecveneto.it

www.aulss8.veneto.it

Gestione del Risk Assessment e del
Data Protection Impact Assessment

Linee guida metodologiche

trasmesse da AZIENDA ZERO

(nota 17.12.2018 prot. 16336) come recepite dall'U.L.SS. n. 8 Berica *(con apposito atto deliberativo)*

INDICE

1 Premessa di carattere organizzativo e metodologico

Ogniqualvolta nel presente documento, a seguito di specifico riferimento normativo, sia indicato quale soggetto il "Titolare del trattamento" si faccia riferimento, per lo svolgimento dei diversi adempimenti, al soggetto e/o alla struttura aziendale individuata dal Titolare del trattamento ratione materiae ed in base all'organizzazione dettata dall'Atto Aziendale.
Ciò detto, al fine di applicare efficacemente le presenti linee guida, ciascuna Azienda, nel caso in cui non lo avesse già fatto, individuerà preliminarmente le strutture aziendali che dovranno concorrere all'attuazione degli adempimenti oggetto del presente documento, in ragione della natura degli adempimenti medesimi *(a titolo esemplificativo e non esaustivo: verranno distinti gli obblighi di carattere giuridico da quelli di carattere tecnologico ed informatico, da quelli afferenti all'area statistica, di internal auditing o di controllo di gestione, etc..)*.

Al fine di dare attuazione alle suesposte indicazioni di Azienda Zero, questa U.L.SS. n. 8 ha approvato l'atto deliberativo del direttore generale ad oggetto: **"Privacy europea: approvazione del nuovo PIANO OPERATIVO DI DISTRIBUZIONE DELLE COMPETENZE all'interno dell'ULSS n. 8 Berica al fine di recepire le indicazioni fornite da Azienda Zero per l'attuazione del GDPR".**

Secondo il "Piano operativo" anzidetto e per quanto concerne l'applicazione delle presenti Linee Guida, le strutture aziendali competenti sono la **UOS Sistemi Informativi, la UOC Controllo di Gestione e il Servizio di Internal Auditing** al quale vengono assegnati compiti e interazioni indicati nell'anzidetto "Piano operativo" a cui si fa espresso ed integrale rinvio.

2 Introduzione e obiettivi del documento

2.1 Introduzione

L'articolo 35 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito GDPR) introduce il concetto di valutazione d'impatto sulla protezione dei dati (in inglese *Data Protection Impact Assessment*, DPIA).

Una valutazione d'impatto sulla protezione dei dati è "*un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli*[1]".

Secondo quanto previsto dall'art. 35, paragrafo 1 del GDPR[2] non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento, ma solo quando il 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".*** Inoltre, ai sensi del sopracitato articolo, una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2.2 Obiettivi del documento

Nell'ambito del contesto sopra descritto, il presente documento ha come obiettivo quello di fornire una guida metodologica per lo svolgimento del *Risk Assessment* (analisi del rischio) sui trattamenti

[1] WP 248, rev. 01 "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, *Working Party* 29 versione 4/10/2017."
[2] Art. 35.1. "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."

posti in essere dall'Azienda ULSS n. 8 Berica (d'ora in avanti "Azienda"), tracciati all'interno del **"Registro delle attività di Trattamento".**

A seguito dell'identificazione dei trattamenti a rischio elevato per i diritti e le libertà degli interessati, il presente documento fornisce, altresì, la guida metodologica per la conduzione del processo di *Data Protection Impact Assessment* su tali trattamenti.

3 Termini e definizioni

Titolare del trattamento (Art. 4, n. 7, del GDPR): 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 di trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Responsabile del trattamento (Art. 4, n. 8, del GDPR): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Interessato: la persona fisica identificata o identificabile **(Art. 4, n. 1, del GDPR)** a cui si riferisce il dato personale oggetto di trattamento.

Dato personale (Art. 4, n. 1, del GDPR): qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Trattamento (Art. 4, n. 2, del GDPR): 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.

Probabilità: valutazione della frequenza con cui il trattamento è effettuato.

Impatto: indicazione della gravità di un incidente che può compromettere la riservatezza, l'integrità e la disponibilità di processi, dati, informazioni incluse nel perimetro di applicazione della normativa *privacy*.

WP29 (Article 29 Working Party o Gruppo di Lavoro Articolo 29 per la protezione dei dati): il gruppo di lavoro comune della autorità nazionali di vigilanza e protezione dei dati. Dal 25 maggio 2018 è stato sostituito dal Comitato europeo per la protezione dei dati (EDPB)

WP 248, rev. 01: "*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*" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018

4 Ambito di applicazione

Ai sensi di quanto disposto dall'art. 35 del GDPR, la valutazione d'impatto sulla protezione dei dati personali è richiesta, in particolare, nei seguenti casi:

a) 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) 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;
c) sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Il punto 4 del predetto art. 35 prevede, inoltre, che l'autorità di controllo rediga e renda pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1.

In adempimento alla norma sopra citata il Garante per la protezione dei dati personali, con provvedimento n. 467 dell'11.10.2018, pubblicato nella Gazzetta Ufficiale il 19/11/2018 (doc.web n. 9058979) ha individuato l'elenco delle tipologie di trattamenti da sottoporre a valutazione d'impatto come di seguito riportato:

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) dai 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

Il Garante nel suddetto documento evidenzia, però, che l'elenco non è esaustivo, essendo riferito esclusivamente a tipologie di trattamento soggette al meccanismo di coerenza da parte del Comitato di cui all'art. 68 del GDPR, e che lo stesso è stato predisposto allo scopo di specificare ulteriormente il contenuto ed a complemento dei criteri individuati dal WP248 rev 01 dello stesso, restando fermo l'obbligo di adottare una valutazione d'impatto sulla protezione dei dati laddove ricorrano due o più criteri individuati dal WP248 rev 01 e che in taluni casi "un titolare del trattamento può ritenere che un trattamento che soddisfa soltanto uno dei predetti criteri richieda una valutazione d'impatto sulla protezione dei dati" [3]

Inoltre, seppure:

- nel documento WP248 rev. 01 il WP29 indichi come non necessaria una valutazione d'impatto sulla protezione dei dati quando:

    - il trattamento non è tale da presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
    - la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è già stata svolta una valutazione d'impatto sulla protezione dei dati;
    - le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018, in condizioni specifiche che non sono mutate;

e

- l'art. 35, paragrafo 10 GDPR disponga che *"Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e) (*cioè qualora la base del trattamento sia un obbligo legale o un interesse pubblico, ndr*), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto 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*

[3] Nel WP248 rev 01 sono individuati i seguenti nove criteri da tenere in considerazione ai fini dell'identificazione dei trattamenti che possono presentare un "rischio elevato": 1) valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"; 2) processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone; 3) monitoraggio sistematico degli interessati; 4) dati sensibili o dati aventi carattere altamente personale; 5) trattamento di dati su larga scala; 6) creazione di corrispondenze o combinazione di insiemi di dati; 7) dati relativi a interessati vulnerabili; 8) uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative; 9) quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto");

generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento",

è vero anche che nei casi in cui non risulti chiara l'obbligatorietà di una valutazione d'impatto sulla protezione dei dati, il WP29 raccomanda di effettuarla ugualmente.

Pertanto si raccomanda di eseguire sempre una valutazione di impatto, sia in quanto non è per lo più noto se una valutazione di impatto generale sia stata eseguita nel contesto dell'adozione della base giuridica di riferimento, sia perché detta valutazione è uno strumento utile in grado di assistere i Titolari del trattamento nella migliore conformazione al GDPR e soprattutto nella migliore dimostrazione dell'accountability, ossia della capacità di dimostrazione di tale conformazione.

5 Rischio *privacy*. Ruoli e responsabilità

La definizione dei ruoli e delle responsabilità dei soggetti coinvolti nelle attività oggetto della presente procedura deve essere effettuata sulla base della struttura organizzativa dell'Azienda sanitaria.

il Titolare svolge la valutazione d'impatto sulla protezione dei dati in collaborazione con il personale di competenza e tramite le strutture aziendali già individuate nel **"PIANO OPERATIVO AZIENDALE DI DISTRIBUZIONE DELLE COMPETENZE"**, a cui si fa espresso ed integrale rinvio.

Nelle linee guida in materia di DPIA del WP29 si legge, infatti, che "*la valutazione d'impatto sulla protezione dei dati può essere effettuata da qualcun altro, all'interno o all'esterno dell'organizzazione, tuttavia al titolare del trattamento spetta la responsabilità ultima per tale compito*".
Ai fini dell'attribuzione di ruoli e responsabilità, si consideri che, ai sensi dell'art. 35, paragrafo 2, del GDPR, è previsto che il Titolare possa consultarsi con il RPD (*quest'ultimo, ai sensi dell'art. 39, paragrafo 1, lettera c, deve sorvegliare lo svolgimento della valutazione d'impatto sulla protezione dei dati*).
A tale proposito, il WP29 ha specificato che "*il parere ricevuto, così come le decisioni prese dal titolare del trattamento, debbano essere documentate all'interno della valutazione d'impatto sulla protezione dei dati*"[4].

Sul punto si segnala, inoltre, che il WP29 raccomanda al Titolare del trattamento di consultare il RPD, fra l'altro, sulle seguenti tematiche[5]:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne, ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- 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.

Qualora il Titolare del trattamento non concordi con le indicazioni fornite dal RPD, occorre che la documentazione relativa alla DPIA riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni.

[4] *Gruppo di Lavoro Articolo 29 per la protezione dei dati, "Linee guida sui responsabili della protezione dei dati" – 16/IT WP243rev.01, adottate il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, pag. 17.*
[5] *Gruppo di Lavoro Articolo 29 per la protezione dei dati, "Linee guida sui responsabili della protezione dei dati" – 16/IT WP243rev.01, adottate il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, pag. 23.*

Nel caso in cui il trattamento sia eseguito in tutto o in parte da un Responsabile del trattamento dei dati, quest'ultimo deve assistere il Titolare del trattamento nell'esecuzione della valutazione d'impatto sulla protezione dei dati e fornire tutte le informazioni necessarie, conformemente all'art. 28, paragrafo 3, lettera f).

6 L'attività di Risk Assessment

L'attività di *Risk Assessment* si sviluppa sulla base dei seguenti step metodologici:

Step 1: Definizione del valore di criticità dei trattamenti
Step 2: Identificazione trattamenti critici.

Nei paragrafi successivi è riportato il dettaglio degli step metodologici previsti ai fini dello svolgimento del *Risk Assessment*.

6.1 Definizione del valore di criticità dei trattamenti

La definizione del valore di criticità dei trattamenti è effettuata partendo dalla mappatura dei trattamenti dei dati personali effettuati dall'Azienda e tracciati all'interno del "Registro delle attività di Trattamento" aziendale.

Nel dettaglio, il contenuto informativo riguarda gli ambiti:
- ID Trattamento
- Direzione/Unità Organizzativa
- Finalità del trattamento
- Base giuridica del trattamento
- Categorie interessati
- Categorie dati personali
- Categoria destinatari a cui i dati personali sono stati o saranno comunicati
- Termine cancellazione dati
- Applicativo o banca dati (cartaceo o elettronico)
- Misure di sicurezza tecniche ed organizzative
- Trattamento verso paese terzo (se previsto) - Paese o organizzazione a cui si invia
- Trattamento verso paese terzo (se previsto) – Garanzie

Per ognuno dei trattamenti mappati, il Titolare del trattamento procede con la valorizzazione qualitativa (SI; NO) di 24 variabili utili per la definizione del livello di criticità dei trattamenti (rif. Allegato 1).

Tali variabili sono classificate nelle seguenti 7 categorie, corrispondenti alle principali determinanti che contribuiscono all'esposizione al rischio di ciascun trattamento:

1 Trattamento categorie particolari di dati
2 Trattamento dati di minori
3 Trattamento su altre categorie di dati
4 Finalità
5 Coinvolgimento soggetti terzi
6 Infrastruttura
7 Utilizzo *device* e/o supporti removibili

A ognuna delle 24 variabili oggetto di valutazione è associato un peso (rif. Allegato 1), espressione del livello di criticità associato alla variabile stessa sulla base della scala di seguito riportata.

Livelli di criticità delle variabili		
Livello di criticità	**Peso delle variabili**	**Descrizione**
ALTO	3	Variabile che può determinare un alto livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un alto impatto sui diritti e sulle libertà delle persone fisiche
MEDIO	2	Variabile che può determinare un medio livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un medio impatto sui diritti e sulle libertà delle persone fisiche
BASSO	1	Variabile che può determinare un basso livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un basso impatto sui diritti e sulle libertà delle persone fisiche

Il valore di criticità del trattamento è ottenuto come somma del peso delle variabili valorizzate con "Sì".

6.2 Identificazione trattamenti critici

Sulla base del valore di criticità determinato, i trattamenti sono classificati in funzione del rispettivo livello di criticità sulla base dell'applicazione dei *range* di seguito riportati:

Livelli di criticità del trattamento			
Livello di criticità	**Descrizione**	**Range per la determinazione del livello di criticità**	**Descrizione range**
ALTO	Il trattamento determina un alto livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un alto impatto sui diritti e sulle libertà delle persone fisiche	$\sum n: k \geq 20$ V $X_1 \geq 1$	Sono considerati trattamenti a criticità **"Alta"** tutti i trattamenti la cui somma delle variabili è maggiore o uguale a 20, o se il trattamento è caratterizzato dalla presenza di almeno una variabile con livello di criticità "3" [6]
MEDIO	Il trattamento determina un medio livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un medio impatto sui diritti e sulle libertà delle persone fisiche	$\sum n: 10 \leq k \leq 19$ V $X_2 \geq 2$	Sono considerati trattamenti a criticità **"Media"** tutti i trattamenti la cui somma delle variabili è compresa tra 10 e 19, o se il trattamento è caratterizzato dalla presenza di almeno due variabili con livello di criticità "2"

[6] Tale criterio, in caso di contrasto, prevale su quello relativo alla somma numerica delle variabili.

BASSO	Il trattamento determina un basso livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un basso impatto sui diritti e sulle libertà delle persone fisiche	∑n: k<10 V X_1=0 X_2<2	Sono considerati trattamenti a criticità **"Bassa"** tutti i trattamenti la cui somma delle variabili è minore di 10, o se il trattamento non è caratterizzato dalla presenza di variabili con livello di criticità "3" e dalla presenza di un numero di variabili con livello di criticità "2" inferiore a 2.

Un trattamento è valutato come "critico" nel caso in cui il Livello di Criticità del Trattamento risulti uguale ad "ALTO".
Per i trattamenti critici identificati, il Titolare del trattamento, effettua la valutazione del rischio per i diritti e le libertà delle persone fisiche scaturente dal trattamento nei seguenti due momenti:

- Valutazione del Rischio Inerente sulla base di criteri di impatto e probabilità;
- Valutazione del Rischio Residuo a seguito della valutazione dei controlli posti in essere ai fini della mitigazione del rischio e corrispondenti al sistema di prevenzione e protezione dei dati personali in essere.

7 L'attività di Data Protection Impact Assessment

L'attività di *Data Protection Impact Assessment* (DPIA) si sviluppa sulla base dei seguenti step metodologici:

Step 1: Valutazione del livello di Rischio Inerente
Step 2: Identificazione tipologia di trattamento
Step 3: Valutazione controlli
Step 4: Definizione del livello di Rischio Residuo
Step 5: Identificazione trattamenti rischiosi

Nei paragrafi successivi si riporta il dettaglio degli step metodologici previsti ai fini dello svolgimento del *Data Protection Impact Assessment*.

7.1 Valutazione del livello di Rischio Inerente

Il *Data Protection Impact Assessment* inizia con la valutazione del Rischio Inerente, attraverso il quale viene identificato il rischio del trattamento, senza considerare gli eventuali presidi di controllo posti in essere dall'Azienda per la sua mitigazione, combinando, sulla base di metriche predefinite, le seguenti due dimensioni:

- **Impatto**, ovvero il possibile effetto che la diffusione dei dati potrebbe avere per l'interessato;
- **Probabilità di accadimento,** ovvero la frequenza con cui il trattamento è effettuato.

Il Titolare del trattamento, valuta qualitativamente l'impatto e la probabilità connessi a ciascun trattamento sulla base dell'applicazione di specifiche scale di valutazione (rif. Allegati 2 e 3).

I valori di Impatto e Probabilità attribuiti sono tradotti quantitativamente su una scala da 1 a 4, dove 1 corrisponde al valore minimo (es. Impatto = Trascurabile; Probabilità = Evento raro) e 4 corrisponde al valore massimo (es. Impatto = Massimo; Probabilità = Evento probabile).

Il Rischio Inerente è calcolato quantitativamente come il prodotto tra i valori di Impatto e Probabilità associati a ciascun trattamento in un *range* da 1 a 16[7].[8]

7.2 Identificazione tipologia di trattamento

Ai fini della valutazione dei controlli previsti nell'ambito dello Step 3, il trattamento è classificato in funzione delle modalità con cui è svolto, in:

- Cartaceo: trattamento effettuato unicamente in modalità cartacea;
- Elettronico: trattamento effettuato unicamente in modalità elettronica;
- Cartaceo/Elettronico: trattamento effettuato in modalità cartacea ed elettronica.

7.3 Valutazione controlli

In seguito all'identificazione della tipologia di Trattamento (cartaceo, elettronico o cartaceo/elettronico), il Titolare del trattamento, effettua la valutazione dei controlli per i trattamenti in funzione della tipologia identificata:

- **Tipologia di trattamento cartaceo**: valutazione dei seguenti 4 controlli, definiti sulla base delle *best-practice* di *Risk Management* e tenendo conto della Metodologia di *Risk Management* ISO 31001, di seguito riportata:

  1 chiara identificazione di ruoli e responsabilità del controllo;
  2 periodico svolgimento delle attività di controllo;
  3 formale definizione dei controlli/ norme comportamentali in policy/procedure aziendali;
  4 presenza di misure di sicurezza fisiche per la gestione del cartaceo (es. presenza armadi/distruggi documenti).

- **Tipologia di trattamento elettronico**: valutazione di 14 controlli, coincidenti con i domini dello standard ISO/IEC 27001/2013, associati a specifici obiettivi in materia di Sicurezza delle Informazioni (rif. Allegato 4) e di seguito riportati:

  1 politiche per la sicurezza delle informazioni;
  2 organizzazione della sicurezza delle informazioni;
  3 sicurezza delle risorse umane;
  4 gestione degli *asset*;
  5 controllo degli accessi;
  6 crittografia;
  7 sicurezza fisica e ambientale;
  8 sicurezza delle attività operative;
  9 sicurezza delle comunicazioni;
  10 acquisizione, sviluppo e manutenzione dei sistemi;
  11 relazioni con i fornitori;
  12 gestione degli incidenti relative alla sicurezza delle informazioni;
  13 *disaster recovery – business continuity*;
  14 *compliance*.

- **Tipologia di trattamento Cartaceo/Elettronico:** valutazione sia dei controlli per i trattamenti

[7] In un'ottica di efficienza operativa la valutazione dei controlli può essere svolta anche solo per i trattamenti il cui valore di Rischio Inerente è maggiore o uguale a 6. I restanti trattamenti sono considerati infatti già a livello Inerente a basso rischio.

[8] Si suggerisce la lettura del documento " Analyse d'impact relative à la protection des donnès : 3. Les bases de connaissance" emesso dalla CNIL, l'Autorità francese per la protezione dei dati (versione in inglese "Privacy Impact Assessment. Knowledge bases")

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf versione francese

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledge bases.pdf versione inglese

cartacei, che dei controlli definiti per i trattamenti elettronici, per un totale di 18 controlli.

Ogni controllo è valutato quantitativamente sulla base di una scala a tre livelli:

- 0: Controllo nullo/assente;
- 0,5: Controllo parzialmente soddisfatto;
- 1: Controllo totalmente soddisfatto.

Ai fini del calcolo del Livello di Controllo, distintamente per le due tipologie di controlli (per trattamenti elettronici/Per trattamenti cartacei) è associato un peso uniforme.
La valutazione del controllo per ogni trattamento è ottenuta come somma ponderata della valutazione associata a ciascun controllo per il relativo peso.
Ai fini della definizione del livello di Rischio Residuo previsto nello step 4, per i Trattamenti effettuati in modalità Cartaceo/Elettronico è considerata la minore tra le valutazioni del controllo associate.

7.4 Definizione del livello di Rischio Residuo

Il valore del Rischio Residuo per ciascun trattamento è definito a partire dal valore di Rischio Inerente e in considerazione del valore del controllo mediante l'applicazione del seguente algoritmo di calcolo:

$$Valore\ Rischio\ Residuo = Valore\ Rischio\ Inerente * (1 - Valutazione\ Controllo)$$

Il valore ottenuto è successivamente ricondotto a una scala qualitativa ad 8 valori (rif. Allegato 5).

7.5 Identificazione trattamenti rischiosi

In considerazione del livello di Rischio Residuo, i trattamenti sono classificati in:

- **Trattamenti a rischio trascurabile**: trattamenti che presentano un valore del Rischio Residuo minore di 4 (corrispondente ai Livelli Trascurabile / Molto-Basso) e per i quali non è necessario indirizzare azioni di adeguamento;
- **Trattamenti a rischio basso**: trattamenti che presentano un valore del Rischio Residuo minore di 8 e maggiore di 4 (corrispondente ai livelli Basso / Medio-Basso) per i quali non è necessario indirizzare azioni di adeguamento, ma è possibile valutare delle azioni per il miglioramento/ottimizzazione del sistema di prevenzione e protezione del rischio;
- **Trattamenti a rischio medio**: trattamenti che presentano un valore di Rischio Residuo minore di 12 e maggiore di 8 (corrispondenti ai livelli Medio / Medio Alto), per i quali è consigliato di individuare e indirizzare azioni di adeguamento e di miglioramento/ottimizzazione del sistema di prevenzione e protezione del rischio;
- **Trattamenti a rischio alto**: trattamenti che presentano un valore del Rischio Residuo maggiore di 12 (corrispondenti ai livelli Alto / Molto Alto), per i quali è necessario individuare e indirizzare azioni di adeguamento e di miglioramento/ottimizzazione del sistema di prevenzione e protezione del rischio. In questo caso il Titolare del trattamento è obbligato a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento.

8 Consultazione Preventiva

Nel caso in cui la valutazione d'impatto sulla protezione dei dati produca come risultato finale che il trattamento presenta un Rischio Residuo elevato (c.d. Trattamenti a Rischio Alto), anche sulla base dei presidi di controllo in essere, il Titolare del trattamento pone in essere le attività necessarie a effettuare una c.d. consultazione preventiva con l'Autorità di controllo.

Ai sensi dell'art. 36, paragrafo 3, del GDPR, la richiesta di consultazione inviata dovrà contenere indicazioni almeno relativamente a:

- ove applicabile, le rispettive responsabilità del Titolare del trattamento, di eventuali contitolari e responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;
- le finalità e mezzi del trattamento previsto;
- le misure e le garanzie previste per la protezione dei diritti e delle libertà degli interessati;
- ove applicabile, i dati del RPD;
- le valutazioni di impatto sulla protezione dei dati dalle quali è risultato un livello di rischio elevato;
- eventuali ulteriori informazioni richieste da parte dell'Autorità di Controllo.

L'Autorità di controllo, entro un termine di otto settimane, al massimo prorogabile di ulteriori sei settimane, fornirà un parere scritto all'interno del quale sarà indicato se ritiene che il trattamento in esame violi i requisiti regolamentari oppure se lo stesso sia in linea con quanto disciplinato dal GDPR.

- ✓ Seguono i n. 5 (cinque) ***documenti tecnici allegati*** al presente documento.

ALLEGATI

Allegato 1 - Variabili oggetto di valutazione e relativi pesi

#	Variabile	Peso della variabile per la determinazione del livello di criticità del trattamento
1	Dati che rivelano l'origine razziale o etnica	**3**
2	Dati che rivelano le opinioni politiche	**3**
3	Dati che rivelano le convinzioni religiose o filosofiche	**3**
4	Dati che rivelano l'appartenenza sindacale	**3**
5	Dati genetici	**3**
6	Dati biometrici	**3**
7	Dati relativi alla salute (Appartenenza a categoria protetta o info su permessi per malattia o info su permessi per Maternità senza visibilità del referto medico)	**2**
8	Dati relativi alla salute (con evidenza del referto medico e/o informazioni su particolari disabilità)	**3**
9	Dati relativi alla vita sessuale o all'orientamento sessuale di una persona	**3**
10	Profilazione e/o *marketing* su minori	**3**
11	Trattamento categorie particolari di dati su minori	**3**
12	Dati di identità per altre finalità	**2**
13	Carte di Credito / CC Bancari	**3**
14	Dati di localizzazione	**1**
15	Dati di Videosorveglianza	**3**
16	Finalità di *marketing* (invio comunicazioni commerciali)	**2**
17	Finalità di profilazione	**3**
18	Presenza di soggetti terzi (fornitori e non) con cui possono essere condivisi i dati	**2**
19	Infrastruttura (di [+] o di fornitori esterni) o parte delle infrastrutture coinvolte nel trattamento in Cloud (Cloud / SaaS)	**2**
20	Infrastruttura (di [+] o di fornitori esterni) o parte delle infrastrutture coinvolte nel trattamento in Cloud (Private Cloud)	**1**
21	*MS Exchange in Private Cloud*	**1**
22	Dati Residenti fuori dall'UE	**3**
23	Dati trattati attraverso l'utilizzo di device portatili (per es. tablet), anche da parte dei dipendenti	**1**
24	Permesso l'utilizzo di supporto removibili per il trasferimento dei dati	**2**

Allegato 2 - Criteri di valutazione dell'Impatto

Criteri di valutazione dell'Impatto		
Valutazione	**Scala**	**Descrizione**
MASSIMO	4	Informazioni che, se divulgate, potrebbero avere delle conseguenze quasi irreversibili per l'interessato: elevati problemi finanziari, problemi fisici e psicologici di lungo termine (es. dettagli giudiziari, dati relativi alla salute etc.).
SIGNIFICATIVO	3	Informazioni che, se divulgate, potrebbero avere significative conseguenze per l'interessato: peggioramento stato di salute, perdita del lavoro, rischio di essere inserito in *black list* (es. morosità esattoriale etc.).
LIMITATO	2	Informazioni che, se divulgate, potrebbero causare all'interessato problemi di carattere personale: danno economico, stress, impossibilità di accedere a determinati servizi/prodotti, lieve danno fisico (es. dettagli note spese, CV, retribuzione, benefit sociali).
TRASCURABILE	1	Informazioni quasi pubbliche che, nel caso fossero divulgate a persone non autorizzate, non creerebbero nessuna problematica all'interessato (es. dati pubblici, numero di telefono fisso privato presente negli elenchi telefonici).

Allegato 3 - Criteri di valutazione della Probabilità di accadimento

Criteri di valutazione della Probabilità di accadimento		
Valutazione	**Scala**	**Descrizione**
EVENTO PROBABILE	4	Il trattamento avviene con frequenza giornaliera (almeno una volta al giorno).
EVENTO POSSIBILE	3	Il trattamento avviene con frequenza settimanale (almeno una volta a settimana).
EVENTO IMPROBABILE	2	Il trattamento avviene con frequenza mensile/ trimestrale (almeno una volta al mese o a trimestre).
EVENTO RARO	1	Il trattamento avviene con frequenza semestrale/ annuale (almeno una volta a semestre/anno).

Allegato 4 - Dettaglio controlli per trattamenti elettronici

#	Dominio ISO/IEC 27001/2013	Obiettivo
1	**Politiche per la sicurezza delle informazioni**	Fornire indicazioni di gestione e supporto per la sicurezza delle informazioni in accordo con i requisiti di *business* e regolamenti cogenti.
2	**Organizzazione della sicurezza delle informazioni**	Stabilire un quadro di gestione per avviare e controllare l'implementazione della sicurezza delle informazioni all'interno dell'organizzazione.
3	**Sicurezza delle risorse umane**	Assicurare che il personale comprenda le proprie responsabilità e sia adeguato al ruolo loro assegnato.
4	**Gestione degli *asset***	Identificare gli *asset* dell'organizzazione e definire appropriate responsabilità per la loro protezione.
5	**Controllo degli accessi**	Prevenire l'accesso di utenti non autorizzati ai sistemi ed alle applicazioni.
6	**Crittografia**	Proteggere la riservatezza, l'autenticità o l'integrità delle informazioni attraverso strumenti di crittografia.
7	**Sicurezza fisica e ambientale**	Prevenire accessi fisici non autorizzati, intromissioni e danni alle infrastrutture informative ed alle informazioni.
8	**Sicurezza delle attività operative**	Assicurare una gestione operativa corretta e sicura delle apparecchiature per l'elaborazione delle informazioni.
9	**Sicurezza delle comunicazioni**	Assicurare la salvaguardia delle informazioni in rete e la protezione dell'infrastruttura di supporto.
10	**Acquisizione, sviluppo e manutenzione dei sistemi informativi**	Assicurare che la sicurezza sia parte integrante dei sistemi informativi in tutto il ciclo di vita. Esso include anche i requisiti per i sistemi informativi che forniscono servizi sulle reti pubbliche.
11	**Relazioni con i fornitori**	Assicurare la protezione degli *asset* dell'organizzazione accessibili ai fornitori.
12	**Gestione degli incidenti relativi alla sicurezza delle informazioni**	Assicurare un approccio efficace e consistente alla gestione degli incidenti di sicurezza informatica, inclusi tutti gli eventi e le vulnerabilità di sicurezza delle comunicazioni.
13	**Disaster Recovery / Business Continuity**	La continuità della sicurezza delle informazioni dovrebbe essere integrata all'interno del sistema di gestione della continuità operativa dell'organizzazione.
14	**Conformità**	Evitare la violazione di obblighi legali, regolamentari o contrattuali relativi alla sicurezza delle informazioni e di eventuali requisiti di sicurezza.

Allegato 5 – Scala di valutazione del livello di Rischio Residuo

		Intervallo Numerico Rischio	
	Livello Rischio Residuo	**Da**	**a**
Trascurabile	Trascurabile	0	2
	Molto - Basso	2	4
Basso	Basso	4	6
	Medio - Basso	6	8
Medio	Medio	8	10
	Medio - Alto	10	12
Alto	Alto	12	14
	Molto - Alto	14	16

***