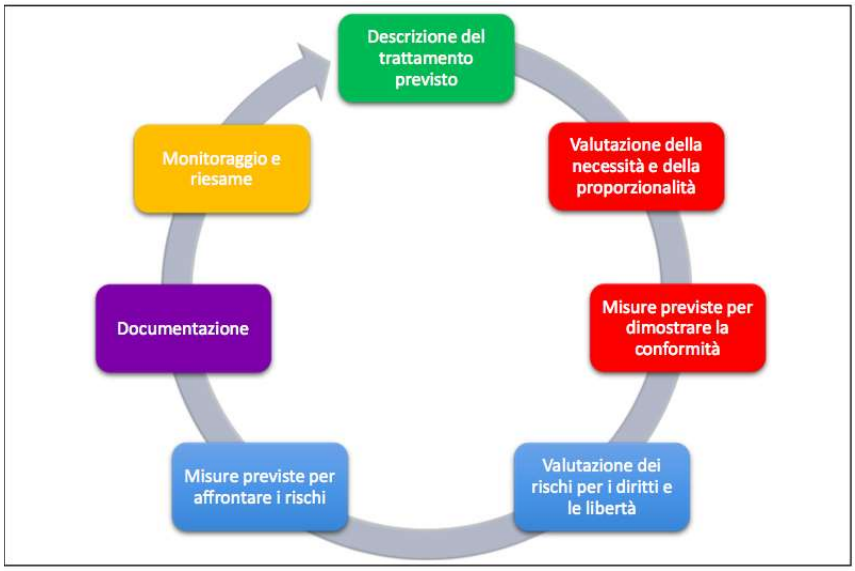
PROCEDURA PER LA GESTIONE DELLE VALUTAZIONI DI IMPATTO PRIVACY (DATA PROTECTION IMPACT ASSESSMENT – DPIA)

SOMMARIO

PREMESSA

Scopo del documento è quello di mettere a disposizione dell'Azienda Sanitaria Locale Torino 4 (di seguito "Azienda" o "ASL TO4") una procedura per lo svolgimento delle valutazioni di impatto sulla protezione dati (Data Protection Impact Assessment, di seguito "DPIA"), prevista come obbligatoria, per i titolari del trattamento dei dati personali, dall'articolo 35 del Regolamento (UE) 2016/679 (General Data Protection Regulation, di seguito "GDPR"), per i trattamenti il cui rischio sia "elevato" per i diritti e le libertà degli interessati nonché per i trattamenti per i quali il legislatore e le autorità di controllo hanno ritenuto, "a monte", necessario lo svolgimento di una DPIA (es. videosorveglianza).
Una prima analisi del rischio-base (Rb) di un trattamento di dati personali viene effettuata mediante il software adottato dall'Azienda per la tenuta del registro dei trattamenti, che consente di capire se è possibile far rientrare il rischio entro una soglia di accettabilità.
Laddove vi sia, invece, evidenza di un rischio "elevato", è necessario procedere allo svolgimento di una DPIA, il cui contenuto è previsto tassativamente nell'art. 35, GDPR.
La presente procedura, dunque, dopo una breve descrizione del contesto normativo di riferimento, illustra come dovrebbe essere condotta una DPIA, in tutte le sue fasi.
La metodologia adottata, proposta da Cap&G s.r.l., Responsabile Protezione Dati (RPD/DPO) pro tempore dell'Azienda, è basata su quella definita dalla Commission nationale de l'informatique et des libertés (CNIL) nel suo software di supporto per lo svolgimento della DPIA ("The open source PIA software helps to carry out data protection impact assessment", url https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment), nonché sulle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati" del Gruppo di lavoro ex art. 29 (WP29).

La figura seguente, presente nelle Linee Guida del Gruppo di lavoro Art. 29 sulla valutazione di impatto sulla protezione dei dati, illustra uno standard del processo per lo svolgimento di una valutazione d'impatto sulla protezione dei dati.



La procedura viene portata a conoscenza dell'Ufficio Privacy (di seguito "UP") nonché dei soggetti Delegati per specifici compiti e funzioni in materia di protezione dati personali, mediante invio del presente documento, nonché attraverso specifiche sessioni formative.

N.B.: tutti i testi in corsivo sono da considerarsi come esempi

1. CONTESTO NORMATIVO

1.1 NORMATIVA E DOTTRINA DI RIFERIMENTO

Regolamento (UE) 2016/679, General Data Protection Regulation, Regolamento Generale Protezione Dati, di seguito GDPR: Artt. 24, 32, 35 e 36; Consideranda 84, 89, 90, 91, 93, 94, 95 e 96;
Linee guida in materia di valutazione d'impatto sulla protezione dei dati (WP248 rev0.1), Gruppo di lavoro ex art. 29 per la protezione dei dati (WP29);
Provvedimento dell'Autorità garante per la protezione dei dati personali dell'11 ottobre 2018, n. 467;
ENISA, Handbook on Security of Personal Data Processing, 2018;
ENISA, On-line tool for the security of personal data processing, at https://www.enisa.europa.eu/risk-level-tool/;
COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL), The open source PIA software helps to carry out data protection impact assessment, https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment;
D. Korff, M. Georges, con il contributo del Garante italiano per la protezione dei dati personali & dei partner del progetto, Manuale RPD - Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europea, versione approvata dalla Commissione, luglio 2019, p. 204 e segg.;
Linee guida sui responsabili della protezione dei dati Adottate il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017 - WP243.rev 01, Gruppo di lavoro ex art. 29 per la protezione dei dati (WP29);
EUROPEAN DATA PROTECTION SUPERVISOR, EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation (case 2020-0066), 2020;
Antonio Ciccia Messina, Profili di criticità e di invalidità delle norme sanzionatrici del GDPR, in Ciberspazio e diritto: rivista internazionale di informatica giuridica, Stem Mucchi Editore, vol. 22, n. 67 (1 - 2021);
(A cura di) R. D'Orazio, G. D. Finocchiaro, O. Pollicino, G. Resta, Codice della privacy e data protection, Giuffrè Francis Lefebvre, Milano, 2021;
R. Bifulco, G. D'Acquisto, Protezione dei dati personali in Italia tra GDPR e codice novellato, G. Giappichelli Editore, 2021;
B. Locoratolo, Il trattamento dei dati personali e la Privacy, Ed. Giuridiche Simone, 2021;
G. Conti, La protezione dei dati personali per titolari e responsabili del trattamento, Maggioli Editore, 2019;
M. Iaselli, Manuale operativo del D.P.O., Maggioli Editore, 2018.

1.2 PERCHÈ E QUANDO SVOLGERE UNA DPIA.

Il Regolamento generale sulla protezione dei dati personali 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito: GDPR) introduce, nella disciplina sul trattamento dei dati personali, il principio di responsabilizzazione (*accountability* nell'accezione inglese) che impone ai Titolari del trattamento - ossia ai soggetti pubblici e privati che trattano dati personali - di assumere comportamenti proattivi per garantire

il rispetto della riservatezza delle persone fisiche e di adottare misure che consentano di dimostrare di aver fatto tutto il necessario per la piena applicazione dell'art. 5, par. 2.
Ai sensi dell'art. 24 GDPR, il titolare del trattamento è tenuto a mettere in atto misure tecniche e organizzative adeguate allo scopo di garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Dette misure devono essere riesaminate e aggiornate qualora necessario.
D'altronde, anche l'art. 32 GDPR impone al titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate allo scopo di garantire un livello di sicurezza adeguato al rischio.
In tal modo si possono anche salvaguardare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di elaborazione.
L'art. 35 GDPR stabilisce, invece, che quando un tipo di trattamento, 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.
In alcuni casi, l'obbligatorietà della DPIA è stata sancita a monte dal legislatore o dalle Autorità di controllo, comme illustrato di seguito.

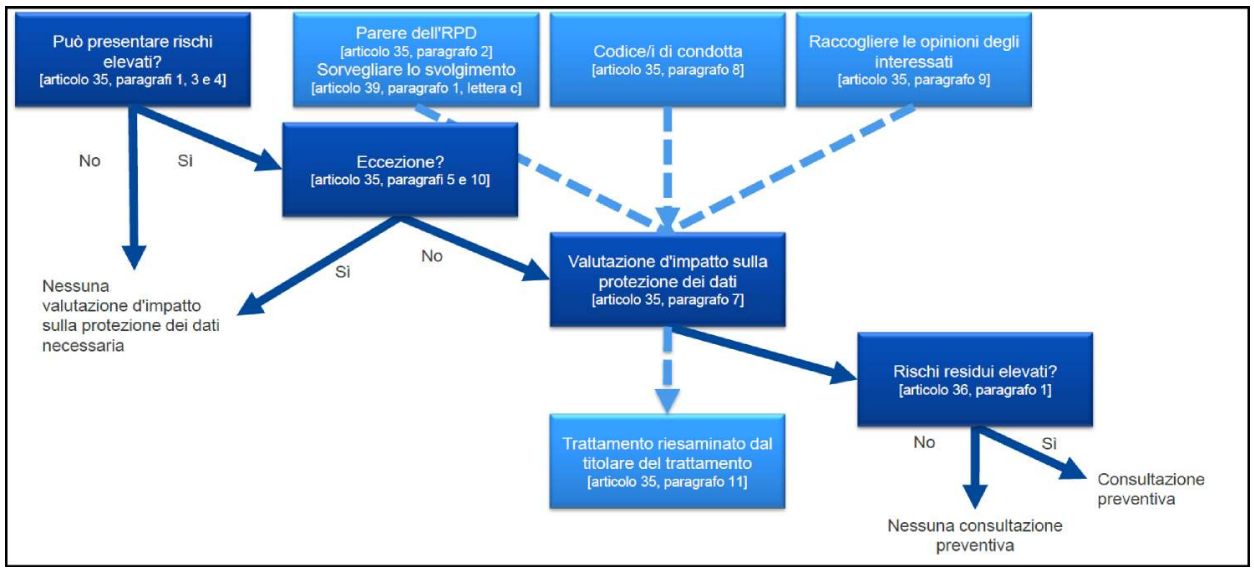
1.3 NORME O DECISIONI DELLE AUTORITÀ CHE RENDONO OBBLIGATORIA LA DPIA

1.3.1 GDPR

Con riguardo all'obbligatorietà della DPIA, l'art. 35, par. 3, GDPR, stabilisce che essa è richiesta in particolare nei casi seguenti:

• 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 di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
• la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Come chiarisce il "Manuale RPD - Linee guida destinate ai RPD nei settori pubblici e parapubblici", in tutti questi casi, e proprio per il fatto che trattamenti di questo tipo comportano rischi intrinsecamente elevati per i diritti e le libertà delle persone, è necessario condurre una Valutazione di impatto sulla protezione dei dati (DPIA), e in determinate circostanze consultare la o le autorità di controllo competenti.



1.3.2 GRUPPO ART. 29

Le Linee guida in materia di valutazione d'impatto del Gruppo di lavoro ex art. 29, allo scopo di dare un ausilio ai titolari nello stabilire quali trattamenti possano presentare un rischio elevato per i diritti e le libertà degli interessati, ha individuato nove criteri:

Valutazione o assegnazione di un punteggio, compresa profilazione
Processo decisionale automatizzato che produce significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni)
Monitoraggio sistematico (es: videosorveglianza)
Dati sensibili, dati giudiziari o dati aventi carattere altamente personale
Trattamento di dati su larga scala
Creazione di corrispondenze o combinazione/raffronto di insiemi di dati
Dati relativi a interessati vulnerabili (minori, soggetti con patologie psichiatriche, anziani, ecc.) che possono non essere in grado di esercitare diritti, acconsentire o opporsi al trattamento
Uso innovativo o applicazione di nuove soluzioni tecnologiche/organizzative
Trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Se ricorrono due o più di questi, il trattamento presenta un rischio elevato, dunque la DPIA è obbligatoria; in presenza di uno soltanto, di questi criteri, la DPIA è consigliata.
Un trattamento può inoltre rientrare in uno di questi criteri ed essere comunque considerato dal Titolare tale da non "presentare un rischio elevato", di conseguenza egli sarà tenuto a documentare questa scelta, includendo il parere del Responsabile Protezione Dati (di seguito "DPO").

1.3.3 GARANTE PRIVACY

L'Autorità Garante per la protezione dei dati personali ha individuato, con il Provvedimento dell'11 ottobre 2018, n. 467, un elenco delle tipologie di trattamenti come potenzialmente suscettibili di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, pertanto, da sottoporre obbligatoriamente a valutazione d'impatto.

Di tale elenco, si elencano di seguito quei trattamenti potenzialmente effettuabili all'Azienda.

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.
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).
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.
Trattamenti su larga scala di dati aventi carattere estremamente personale: 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).
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).
Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
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*) ogni qualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01.
Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
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*).
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.
Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

1.3.4 CNIL

Anche l'autorità di controllo francese ha voluto dare un ausilio ai titolari del trattamento sul tema dell'obbligatorietà della DPIA pubblicando, nel 2019, un elenco di trattamenti, che per loro natura, ambito, contesto e finalità, non richiedono la redazione di una valutazione di impatto.
Tra questi, compaiono:

Trattamenti per la sola gestione delle risorse umane per le organizzazioni con meno di 250 dipendenti, in particolare, per le finalità che riguardano: la gestione della retribuzione e l'emissione delle buste paga; la gestione della formazione; la gestione della mensa aziendale e l'emissione di buoni pasto; il rimborso delle spese professionali; il controllo dell'orario di lavoro; i resoconti delle interviste di valutazione annuali; la tenuta dei registri obbligatori per legge; l'uso di strumenti di comunicazione che non prevedono la profilazione o l'impiego di dati biometrici.
Trattamenti che includono i processi di gestione della relazione con il fornitore di servizi. Nello specifico, per tutte quelle finalità che consentono: di svolgere operazioni amministrative relative a contratti, controlli, ricevimenti, fatture, regolamenti e contabilità per la gestione dei debiti; per creare documenti di pagamento come bozze, assegni e cambiali; per elaborare statistiche finanziarie e sul fatturato per fornitore; di gestire selezioni di fornitori per le esigenze dell'azienda o dell'organizzazione; di conservare la documentazione del fornitore.
Trattamenti relativi all'elaborazione di dati sanitari necessaria per la cura di un paziente da parte di un professionista della salute che pratica individualmente in uno studio medico, un dispensario di farmacia o un laboratorio di biologia medica. In particolare, non sono soggetti a DPIA i trattamenti che regolano: la gestione degli appuntamenti; la gestione delle cartelle cliniche e la redazione delle prescrizioni; la gestione e la conservazione dei file necessari per il follow-up del paziente; l'istituzione e la trasmissione telematica dei fogli di cura; le comunicazioni tra professionisti identificati coinvolti nella cura della persona interessata; la tenuta dei conti.
Trattamenti attuati dalle autorità locali e da soggetti giuridici di diritto pubblico e privato per gestione dei servizi a scuola, extracurriculari e della prima infanzia.
Trattamenti effettuati esclusivamente allo scopo di gestire i controlli e gli orari di accesso fisico per il calcolo dell'orario di lavoro. Nel caso vengano impiegati dispositivi biometrici e trattati dati di categorie particolari allora è necessario procedere alla redazione della DPIA.

1.3.5 ICO: ESEMPI DI ELABORAZIONE "CHE PUÒ COMPORTARE UN RISCHIO ELEVATO"

Anche l'ICO, autorità di controllo del Regno Unito, ha stilato un elenco basato sulle Linee guida WP29, che viene integrato e specificato ulteriormente.
In tale elenco compaiono:

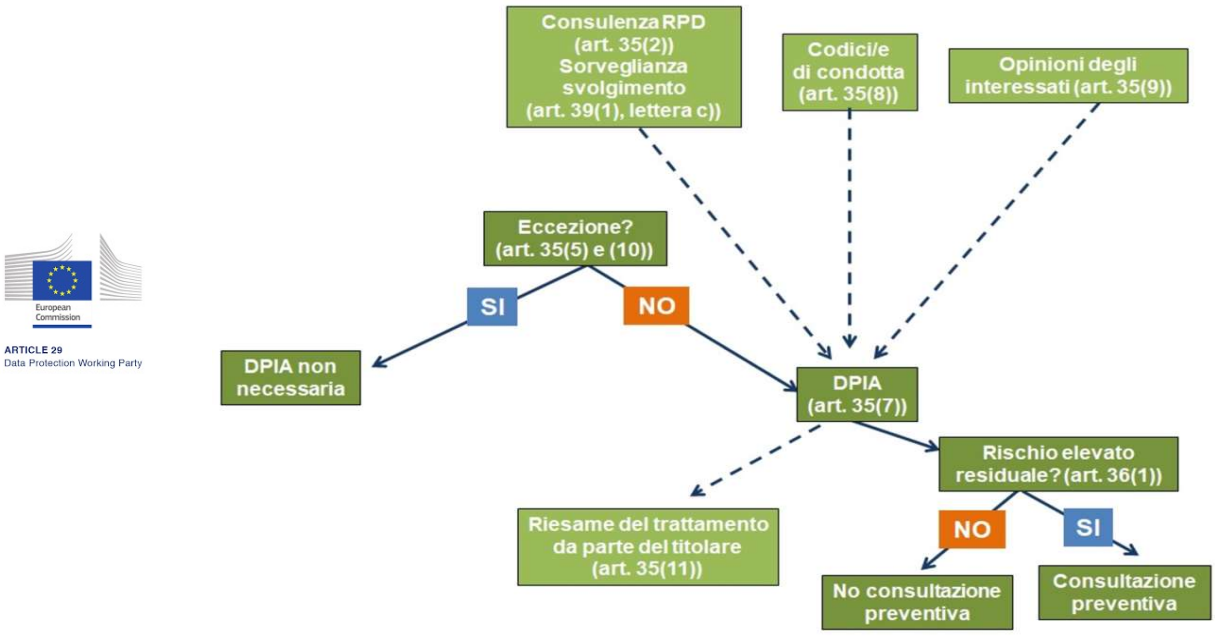
Tipo di operazioni che richiedono una DPIA	**Descrizione**	**Esempi non esaustivi di aree di applicazione esistenti**
Tecnologia innovativa	Elaborazione che prevede l'uso di nuove tecnologie o la nuova applicazione di tecnologie esistenti (compresa l'IA). È richiesta una DPIA per qualsiasi operazione di elaborazione prevista	Intelligenza artificiale, apprendimento automatico e apprendimento profondo Veicoli connessi e autonomi Sistemi di trasporto intelligenti Tecnologie intelligenti

	che implichi un uso innovativo delle tecnologie (o l'applicazione di nuove soluzioni tecnologiche e / o organizzative) se combinato con qualsiasi altro criterio di WP248rev01.	(compresi i dispositivi indossabili) Ricerche di mercato che coinvolgono la neuro-misurazione (ovvero analisi della risposta emotiva e attività cerebrale) Alcune applicazioni IoT, a seconda delle circostanze specifiche dell'elaborazione
Profilazione su larga scala	Qualsiasi profilazione di individui su larga scala	Dati elaborati da Smart Meters o applicazioni IoT Hardware / software che offre monitoraggio del fitness / stile di vita Reti di social media Applicazione dell'IA ai processi esistenti
Dati biometrici	Qualsiasi trattamento di dati biometrici allo scopo di identificare in modo univoco un individuo. È richiesta DPIA per qualsiasi operazione di elaborazione prevista che coinvolga dati biometrici allo scopo di identificare in modo univoco un individuo, se combinato con qualsiasi altro criterio di WP248rev01	• Sistemi di riconoscimento facciale • Sistemi di accesso al posto di lavoro / verifica dell'identità • Controllo degli accessi / verifica dell'identità per hardware / applicazioni (incluso riconoscimento vocale / impronta digitale / riconoscimento facciale)
Dati genetici	Qualsiasi trattamento di dati genetici, diverso da quello elaborato da un singolo medico di famiglia o professionista sanitario per la fornitura di assistenza sanitaria direttamente all'interessato. È richiesta una DPIA per qualsiasi operazione di elaborazione prevista relativa a dati genetici se combinata con qualsiasi altro criterio di WP248rev01	Diagnosi medica Test del DNA Ricerca medica
Rischio di danni fisici	Laddove il trattamento sia tale che una violazione dei dati personali potrebbe compromettere la salute [fisica] o la sicurezza delle persone.	• Procedure di denuncia / denuncia • Registri di assistenza sociale

1.4 COSA DEVE CONTENERE LA DPIA

L'art. 35, par. 7, GDPR stabilisce che la DPIA deve contenere almeno:

• una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
• una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
• una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1 le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.



1.5 LE SANZIONI

Infine, sotto il profilo sanzionatorio, è opportuno ricordare che il mancato svolgimento della DPIA, ove obbligatorio, o lo svolgimento non corretto, o la mancata consultazione dell'autorità di controllo competente, ove ciò sia necessario, possono comportare una sanzione amministrativa pecuniaria, a carico del titolare, fino a un massimo di 10 milioni di Euro, ovvero – se si tratta di un'impresa – fino al 2% del fatturato mondiale totale annuo dell'esercizio finanziario precedente, se superiore.

2. DPIA

2.1 FASI DELLA DPIA E SOGGETTI CHE INTERVENGONO NELLA PROCEDURA

La DPIA deve essere svolta dal Titolare del trattamento, che ha facoltà di decidere quali soggetti intervengono nella DPIA.
Di seguito, sono illustrate le fasi della DPIA, le attività di ciascuna fase e i soggetti che vi intervengono.

Fase	**Attività**	**Allegato corrisp.**	**Autore**
1. Valutazione applicazione principi fondamentali	Descrizione del trattamento, valutazione dell'applicazione dei principi fondamentali.	All. 1	*Soggetto Delegato dell'U.O. di riferimento (Direttore di Struttura) con il supporto del membro del Gruppo di lavoro Privacy competente.*
2. Misure di sicurezza.	Acquisizione delle misure in essere. Valutazione delle singole misure.	All. 2	*UP, con il supporto del DPO e della Funzione informatica.*
3. Valutazione Ri.	Verifica e valutazione del rischio inerente (Ri)	All. 3	*UP, con il supporto del DPO*
4.1 Revisione.	Piano di azione che prevede le azioni correttive, la relativa tempistica e i soggetti responsabili.	All. 4.1	*UP, con il supporto della Funzione informatica/Ingegneria clinica/Fornitori*
4.2 Calcolo del Rischio residuo (Rr)	Attestazione dell'esito del Piano di Azione e Calcolo del Rischio residuo (Rr)	All. 4.2	*UP*
5. Parere.	Parere del DPO sul corretto svolgimento della DPIA.	All. 5	DPO
6. Validazione.	Valutazione del parere del DPO e dell'esito della consultazione degli Interessati; validazione delle misure di sicurezza tecniche ed organizzative prescelte, dell'efficacia del Piano di Azione e dell'accettabilità del rischio residuo (Rr).	All. 6	Direttore Generale/Direttore Amm.vo
7. Aggiornamento periodico / Osservazioni	Aggiornamento periodico / Osservazioni	All. 7	Direttore di S.C./UP

Oltre ai soggetti richiamati, possono intervenire nella procedura:

- Eventuali **Contitolari**. Qualora il trattamento coinvolga diversi soggetti che operano quali Contitolari, questi ultimi devono aver preliminarmente definito con precisione le rispettive competenze nonché gli obblighi spettanti a ciascuno. Allegare la relativa documentazione.

• **Interessati** (o loro rappresentanti), i quali, ai sensi dell'art. 35, par. 9, GDPR, se del caso, devono essere interpellati, dal Titolare del trattamento per la raccolta delle loro opinioni o dei loro rappresentanti sul trattamento oggetto della DPIA. L'esito dell'eventuale consultazione degli Interessati deve essere allegato alla DPIA. È necessario indicare se sono state raccolte le opinioni degli interessati e/o dei rappresentanti degli interessati prima o durante la DPIA.
• Eventuali **soggetti esterni** di cui intende avvalersi il Titolare del trattamento qualora siano richieste competenze specialistiche (es. competenze informatiche, nel campo dell'IA, aspetti relativi al FSE, in materia di videosorveglianza, ecc.).

2.2 PARERE PREVENTIVO DEL DPO

Ai sensi dell'art. 35, par. 2, GDPR, il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il Responsabile Protezione Dati, qualora ne sia designato uno.
Il Gruppo di lavoro WP29, nelle sue Linee guida sui responsabili della protezione dei dati, ha raccomandato che il titolare del trattamento si consulti con il Responsabile Protezione Dati (DPO), fra l'altro, sui seguenti temi:

• **se condurre o meno una DPIA** (che potrebbe non essere necessaria) Alla luce degli esiti dell'analisi del rischio – base risultante dal software del registro dei trattamenti, l'Ufficio privacy richiede, dunque, al Responsabile Protezione Dati (DPO) di formulare un elenco di trattamenti (o di insiemi di trattamenti) da sottoporre a DPIA, mediante apposito parere, che non è vincolante ma è comunque obbligatorio. Qualora il Titolare del trattamento voglia discostarsi dal parere del DPO deve motivare e documentare tale scelta.
• **quale metodologia adottare nel condurre una DPIA e se condurre la DPIA con le risorse interne, ovvero esternalizzandola** La metodologia risiede nella presente procedura, adottata anche con il supporto del DPO.
• **quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate** Il DPO, ove richiesto, può fornire supporto in tutte le fasi della DPIA.
• **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** Mediante parere formale, prima della validazione della DPIA, il DPO attesta la conformità della valutazione di impatto alla normativa vigente.

2.3 FASE 1 - DESCRIZIONE DEL TRATTAMENTO, VALUTAZIONE DELL'APPLICAZIONE DEI PRINCIPI FONDAMENTALI.

Ai sensi dell'art. 35, par. 7, GDPR, il primo elemento della DPIA è la descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, da svolgersi, a cura del Soggetto Delegato dell'U.O. di riferimento (Direttore di Struttura) con il supporto del

membro del Gruppo di lavoro Privacy competente, mediante la compilazione della seguente tabella[1], mutuata dai criteri suggeriti dall'Autorità di controllo francese, CNIL, che ha messo a disposizione sul proprio sito istituzionale un software di ausilio ai titolari in vista della effettuazione della valutazione d'impatto sulla protezione dei dati (DPIA).

Trattamento in considerazione Descrivere il trattamento, le sue principali caratteristiche e l'eventuale processo nell'ambito del quale si inserisce.
Responsabilità connesse al trattamento Descrivere i soggetti coinvolti nel trattamento, definendone ruoli e responsabilità situazioni di titolarità o con titolarità, eventuali Responsabili nominati ai sensi dell'art. 28 GDPR, soggetti Delegati/Autorizzati che hanno accesso ai dati.
Standard applicabili al trattamento
Categorie di dati trattati Indicare le categorie dei dati trattati (dati comuni, dati particolari, dati relativi a condanne penali e reati)
Ciclo di vita del trattamento dei dati Effettuare una descrizione funzionale del ciclo di vita dei dati trattati, dalla raccolta alla cancellazione
Risorse di supporto ai dati
Eventuali destinatari dei dati (con specifico riferimento ad eventuali Titolari Autonomi)

Il secondo elemento necessario della DPIA è la valutazione dei principi fondamentali di necessità, proporzionalità e trasparenza del trattamento in relazione alle finalità.
È necessario, infatti, che il Soggetto Delegato dell'U.O. di riferimento (Direttore di Struttura), con il supporto del membro del Gruppo di lavoro Privacy competente, verifichi che:
- le finalità del trattamento siano determinate, esplicite e legittime (articolo 5, par. 1, lett. b), GDPR)
– il trattamento sia lecito, dunque le sue basi giuridiche (articolo 6 GDPR)
– i dati personali siano adeguati, pertinenti e limitati a quanto necessario (articolo 5, par. 1, lett. c), GDPR)
– i tempi di conservazione siano limitati (articolo 5, paragrafo 1, lett. e), GDPR)
- l'esercizio dei diritti degli interessati sia garantito (articoli 12-22 GDPR)
– i rapporti con i responsabili del trattamento siano disciplinati (articolo 28 GDPR)
– le garanzie riguardanti trasferimenti di dati al di fuori dell'UE o a organizzazioni internazionali siano soddisfatte (capo V GDPR)
– la consultazione preventiva sia svolta, ove necessario (articolo 36 GDPR, che impone al titolare, dopo aver eseguito la valutazione di impatto, di decidere se iniziare il trattamento o consultare l'autorità di controllo competente per avere indicazioni su come gestire il rischio residuale).
Tale attività si svolge secondo la WP 248/2017, come indicato nella seguente tabella[2].

Scopi del trattamento. Indicare se le finalità del trattamento sono determinate, esplicite e legittime (art. 5, par. 1, lett. b) GDPR).
Basi giuridiche. Indicare le basi giuridiche che rendono lecito il trattamento (artt. 6, 9 e 10 GDPR).

[1] Cfr. All. 1
[2] Cfr. All. 1.

Adeguatezza, pertinenza e limitatezza dei dati raccolti. Indicare in che modo è rispettato il principio di minimizzazione, in relazione alle finalità per cui i dati sono trattati. A tal fine si presti attenzione a: quantità di dati raccolti, tipologia, necessità rispetto agli obiettivi del trattamento (art. 5, par. 1, lett. c) GDPR).
Esattezza e aggiornamento dei dati. Indicare se i dati sono esatti e aggiornati nonché le misure adottate a tal fine.
Tempi di conservazione. Indicare la data retention per ciascuna finalità nonché i motivi per cui si ritiene che tale periodo sia necessario al raggiungimento delle specifiche finalità indicate (art. 5, par. 1, lett. e) GDPR).
Esercizio dei diritti degli interessati Indicare come vengono garantiti i diritti degli interessati.
Rapporti con i responsabili del trattamento Indicare come vengono disciplinati i rapporti con i responsabili del trattamento.
Garanzie riguardanti trasferimenti di dati al di fuori dell'UE o a organizzazioni internazionali

N.B. La DPIA potrebbe evidenziare che il trattamento non può essere svolto in quanto non conforme a un principio del GDPR (per esempio, il trattamento può risultare privo di base legale). In tali ipotesi, il trattamento non può essere avviato finché non si è sanata la situazione di non conformità (nell'esempio, fino alla definizione di un'adeguata base legale, previa, se del caso, la consultazione del Garante della protezione dei dati personali ai sensi dell'art. 36, par. 4, GDPR).

L'esito dei controlli della Fase 1 deve essere sintetizzato sia in maniera descrittiva sia in una tabella come quella di seguito riportata, in cui si valuta l'applicazione dei singoli princìpi selezionando la casella corrispondente:
Non accettabile (N – colore rosso);
Migliorabile (M – colore giallo);
Accettabile (A - colore verde).

PRINCIPIO	N	M	A
PF1 - Finalità e basi giuridiche del trattamento			
PF2 - Adeguatezza, pertinenza, limitatezza dei dati			
PF3 - Esattezza e aggiornamento dei dati			
PF4 - Periodo di conservazione dei dati			
PF5 - Informativa ed eventuale raccolta del consenso			
PF6 - Diritti degli interessati			
PF7 - Responsabili del trattamento			
PF8 - Trasferimenti di dati personali al di fuori dell'UE			

2.4 FASE 2 - MISURE DI SICUREZZA

La DPIA procede con l'acquisizione, a cura dell'UP, delle misure di sicurezza tecniche e organizzative esistenti presso l'Azienda per il trattamento sottoposto a valutazione di impatto (qualora il trattamento venga effettuato per il tramite di un Responsabile del trattamento ai sensi dell'art. 28 GDPR, l'UP acquisisce le misure dalla nomina o CCT stipulate).

Conseguentemente, l'UP procede alla valutazione delle singole misure di sicurezza, verificando se nella propria organizzazione è rispettato lo standard di accettabilità di ciascuna misura, e flaggando, per ciascuna misura, la casella corrispondente a:
Non accettabile (N – colore rosso)
Migliorabile (M – colore giallo)
Accettabile (A - colore verde)
come nella tabella che segue[3].

ID	MISURA DI SICUREZZA	N	M	A
MS1	Politiche di tutela della privacy			
MS2	Gestione del "rischio privacy" (specifico per gli Interessati)			
MS3	Politiche di cybersecurity e analisi delle vulnerabilità			
MS4	Gestione del personale (formazione, ruoli e responsabilità, gestione di eventi imprevisti)			
MS5	Gestione relazione con le terze parti che accedono ai dati			
MS6	Vigilanza (audit di conformità)			
MS7	Prevenzione da danni fisici e fonti di rischio non umane			
MS8	Antiintrusione e controllo degli accessi fisici			
MS9	Lotta contro il malware			
MS10	Sicurezza dei siti web			
MS11	Sicurezza di server, reti, Wi-Fi			
MS12	Sicurezza di hardware, postazioni e dispositivi			
MS13	Sicurezza dei software			
MS14	Manutenzione			
MS15	Backup e Restore			
MS16	Business continuity			
MS17	Disaster recovery			
MS18	Controllo degli accessi logici, autenticazione, password			
MS19	Gestione dei profili di accesso			
MS20	Tracciabilità (Logging) degli eventi e monitoraggio integrità dei dati			
MS21	Minimizzazione dei dati			
MS22	Altre misure applicate ai dati			
MS23	Archiviazione e dismissione sicura			
MS24	Archiviazione e dismissione sicura dei documenti su carta			

L'elenco delle misure è elaborato sulla base della normativa e della prassi vigenti.
Per ciascuna misura, nell'allegato 2, sono enuclueate sottomisure efficaci.
Allo scopo di mitigare il rischio del trattamento (che verrà calcolato nella fase 3), tutte quelle misure valutate come "migliorabile" o come "non accettabile" saranno oggetto di azioni correttive nel prosieguo della DPIA.

2.5 FASE 3 – VERIFICA E VALUTAZIONE DEL RISCHIO INERENTE (RI)

[3] Cfr. All. 2.

Il rischio inerente o potenziale (Ri) è il rischio calcolato prima dell'applicazione delle misure di sicurezza.

Rischio inerente = Probabilità (Minaccia) * Gravità (Impatto)
Ri = P * G

Il risultato corrisponde a una scala di valori: potremo avere un rischio inerente (Ri) trascurabile, limitato, importante, massimo.

La DPIA, dunque, in tale frangente, prevede la "verifica":

- **delle fonti di rischio**, che possono essere umane (persona, interna o esterna all'Ente, che opera in via accidentale o intenzionale ad esempio: amministratore IT, utente, attaccante esterno, concorrente, etc.) o non umane (fenomeni climatici, materiali infiammabili o pericolosi, virus informatici, etc.);
- **della natura e della particolarità dei rischi**;
- **delle minacce che possono concretizzare il rischio** (una minaccia è qualsiasi circostanza o evento che ha il potenziale per influire negativamente sulla sicurezza dei dati personali).

Fatto ciò, si passa alla "valutazione" dei rischi per i diritti e le libertà degli interessati, procedendo, in particolare, dalla prospettiva degli interessati mediante una stima di:

- **probabilità (P)** che si verifichino eventi che potrebbero determinare accesso illegittimo, modifica indesiderata, perdita dei dati, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure esistenti;
- **gravità (G)** dei rischi, ossia gli impatti potenziali per i diritti e le libertà degli interessati, nei casi di accesso illegittimo, modifica indesiderata, perdita dei dati.

Per calcolare la gravità degli impatti si può fare riferimento alla seguente legenda.

LIVELLO	Impatto fisico	Esempio	Impatto materiale	Esempio	Impatto psicologico	Esempio
Trascurabile	Gli interessati potrebbero incontrare qualche inconveniente fisico, superabile senza difficoltà.	Mal di testa passeggero.	Gli interessati potrebbero incontrare qualche inconveniente materiale, superabile senza difficoltà.	Perdita di tempo dovuta a ripetizione delle procedure o all'attesa della loro effettuazione, riutilizzo dei dati a scopo di pubblicità mirata per beni di consumo corrente.	Gli interessati potrebbero incontrare qualche inconveniente psicologico, superabile senza difficoltà.	Semplice fastidio, impressione di violazione della privacy senza danno reale (intrusione commerciale).
Limitato	Gli interessati potrebbero sperimentare inconvenienti fisici	Malattia lieve a seguito del mancato rispetto di controindicazi	Gli interessati potrebbero avere inconvenienti materiali,	Pagamenti non pianificati (ad esempio multe non dovute), negazione dell'accesso a servizi amministrativi	Gli interessati potrebbero avere inconvenienti	Disturbo psicologico minore ma oggettivo, senso di violazione

	superabili nonostante alcune difficoltà.	oni, diffamazione che dia luogo a rappresaglie fisiche.	superabili nonostante alcune difficoltà.	o commerciali, pubblicità online mirata su un aspetto di vita privata che la persona voleva mantenere riservata.	psicologici, superabili nonostante alcune difficoltà.	della privacy senza danni irreparabili, intimidazione sui social network.
Importante / Significativo	Gli interessati potrebbero subire conseguenze fisiche significative, che dovrebbero essere in grado di superare, ma con notevoli difficoltà.	Aggravamento dello stato di salute a seguito di una errata assunzione di responsabilità o del mancato rispetto di controindicazioni, alterazione dell'integrità fisica.	Gli interessati potrebbero subire conseguenze materiali significative, che dovrebbero essere in grado di superare, ma con notevoli difficoltà.	Perdite monetarie non indennizzate, perdita di opportunità uniche e non ricorrenti (mutui immobiliari, studi, occupazioni, esami scolastici), perdita dell'abitazione, del posto di lavoro.	Gli interessati potrebbero subire conseguenze psicologiche significative, che dovrebbero essere in grado di superare, ma con notevoli difficoltà.	Grave disturbo psicologico (depressione, fobie), senso di violazione della privacy e di un danno irreparabile, esposizione a ricatti, cyberbullismo e molestie psicologiche.
Massimo	Gli interessati potrebbero sperimentare gravi conseguenze fisiche, anche irrimediabili, che potrebbero non superare.	Affezione fisica a lungo termine o permanente, alterazione permanente dell'integrità fisica, decesso.	Gli interessati potrebbero subire gravi conseguenze materiali, anche irrimediabili, che potrebbero non superare.	Rischio finanziario, indebitamento ingente, impossibilità di lavorare, incapacità di ricollocazione, smarrimento di elementi di prova nell'ambito di un contenzioso, perdita di accesso a infrastrutture vitali (acqua, elettricità, ecc.).	Gli interessati potrebbero subire gravi conseguenze psicologiche, anche irrimediabili, che potrebbero non superare.	Disturbo psicologico a lungo termine, sanzione penale, allontanamento, perdita di legami familiari, perdita capacità di agire, cambio di stato amministrativo e/o perdita dell'autonomia legale (tutela).

La stima, alla luce del metodo CNIL, si realizza compilando i campi presenti nella tabella seguente[4].

Accesso illegittimo ai dati	
Potenziali impatti sugli interessati se il rischio si dovesse concretizzare.	*Esempio: selezionare impatti da tabella precedente*
Principali minacce che potrebbero concretizzare il rischio.	*Esempio: virus informatico*
Fonti di rischio.	*Esempio: mancato aggiornamento del SO, mancanza di firewall e/o antivirus sul pc, ecc.*
Misure che contribuiscono a mitigare il rischio.	*Esempio: selezionare tra le misure di cui all'Allegato 2*
Stima della gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure esistenti.	*Esempio: IMPORTANTE*
Stima della probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure esistenti.	*Esempio: LIMITATA*
Modifiche indesiderate dei dati	

[4] Cfr. All. 3.

Potenziali impatti sugli interessati se il rischio si dovesse concretizzare.	*Esempio: selezionare impatti da tabella precedente*
Principali minacce che potrebbero concretizzare il rischio.	*Esempio: errore del soggetto autorizzato nel modificare i dati*
Fonti di rischio.	*Esempio: mancata formazione dei soggetti che intervengono nel trattamento, ecc.*
Misure che contribuiscono a mitigare il rischio.	*Esempio: selezionare tra le misure di cui all'Allegato 2*
Stima della gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure esistenti.	*Esempio: Il rischio è LIMITATA*
Stima della probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure esistenti.	*Esempio: Il rischio è LIMITATA*
Perdita dei dati	
Potenziali impatti sugli interessati se il rischio si dovesse concretizzare.	*Esempio: selezionare impatti da tabella precedente*
Principali minacce che potrebbero concretizzare il rischio.	*Esempio: ransomware e conseguente impossibilità di utilizzo dei servizi*
Fonti di rischio.	*Esempio: Falla nella sicurezza, mancata formazione dei soggetti che intervengono nel trattamento*
Misure che contribuiscono a mitigare il rischio.	*Esempio: selezionare tra le misure di cui all'Allegato 2*
Stima della gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure esistenti.	*Esempio: Il rischio è LIMITATA*
Stima della probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure esistenti.	*Esempio: Il rischio è LIMITATA*

La stima dei valori probabilità (P) e gravità (G) per accesso (a), modifica (m) e perdita (p) dei dati, può essere sintetizzata graficamente in una immagine come nell'esempio seguente, in cui i punti rossi rappresentano i valori del rischio inerente (Rr).

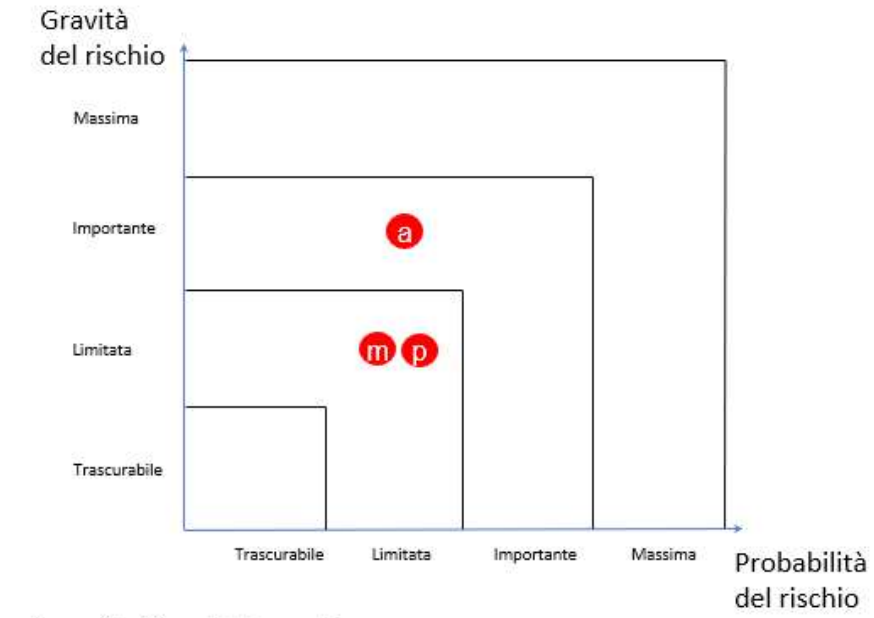


Grafico della valutazione del Rischio Inerente (Ri)
ossia il rischio prima dell'attuazione del Piano di Azione (finalizzato al miglioramento di alcune misure di sicurezza)

(TABELLA DI ESEMPIO)

2.6 FASE 4 – REVISIONE E CALCOLO DEL RISCHIO RESIDUO (RR).

Come indicato in precedenza, la presente metodologia si sviluppa sulla base di quella definita dalla Commission nationale de l'informatique et des libertés (CNIL).
Dunque, conclusa la fase della DPIA in cui si è calcolato il Rischio inerente o potenziale (Ri, precedente all'applicazione delle misure di sicurezza), si passa alla fase della Revisione.
Infatti, lo scopo della procedura è quello di determinare misure aggiuntive (laddove venga rilevato che lo standard di accettabilità della misura non sia rispettato) finalizzate a mitigare il rischio inerente (Ri) (art. 35, par. 7, lett. d), GDPR e Cons. 90, GDPR).

Nella fase di Revisione, dunque, è necessario:
1) **individuare**, per quelle misure valutate come MIGLIORABILE o come NON ACCETTABILE, alcune **possibili azioni correttive** da adottare al fine di mitigare il rischio inerente (Ri), definendo le tempistiche e le responsabilità connesse per l'implementazione di tali azioni[5], come nell'esempio di seguito riportato.

Piano di azione

ID MISURA	*MISURA AGGIUNTIVA O CORRETTIVA*	*TERMINE*	*RESPONSABILE DELL'ATTUAZIONE*
MS6	***Vigilanza (audit di conformità)*** • *è necessario adottare una Procedura di audit, interni ed esterni, che consenta di avere una visione globale e aggiornata dello stato di protezione dei dati e della conformità con*	*15/06/2024*	*UP, con il supporto del DPO*

[5] Cfr. All. 4.1

	il GDPR, allo scopo di condurre verifiche ispettive interne ed esterne sul campo, nonché adottare e documentare misure che consentano di assicurare l'effettività delle garanzie offerte dai responsabili del trattamento in materia di protezione dei dati.		
MS13	***Sicurezza dei software*** • *Predisporre un inventario dei software in uso*	*15/06/2024*	*UP, con il supporto della Funzione Informatica*

2) **attestare l'esito del Piano di Azione** (ossia se le azioni correttive sono state attuate nei tempi previsti, con motivazione) e **valutare il rischio residuo (Rr)** del trattamento[6] (che è il rischio inerente (Ri) una volta mitigato grazie alle azioni correttive), sintetizzabile con la seguente formula:

Rischio residuo = Probabilità (Minaccia) * Gravità (Impatto) / Efficacia (Misure aggiuntive o correttive)

$$Rr = \frac{P * G}{E}$$

Dunque, come già fatto in precedenza, per ciascun evento accesso (a), modifica (m) e perdita (p) dei dati, si potrà valutare il rischio residuo (Rr) del trattamento sosttoposto a DPIA, come nell'esempio seguente.

Alla luce del piano d'azione, la **gravità** del rischio di **Accesso illegittimo ai dati** sarà:
Limitata
Alla luce del piano d'azione, la **probabilità** del rischio di **Accesso illegittimo ai dati** sarà:
Trascurabile
Il rischio di **Accesso illegittimo ai dati** si pone dunque nell'area *LIMITATA (poiché viene rilevato il valore più grande tra gravità e probabilità)*

Alla luce del piano d'azione, la **gravità** del rischio di **Modifiche indesiderate ai dati** sarà:
Trascurabile
Alla luce del piano d'azione, la **probabilità** del rischio di **Modifiche indesiderate ai dati** sarà:
Trascurabile
Il rischio di **Modifiche indesiderate ai dati** si pone dunque nell'area *TRASCURABILE*

Alla luce del piano d'azione, la **gravità** del rischio di **Perdita dei dati** sarà:
Trascurabile
Alla luce del piano d'azione, la **probabilità** del rischio di **Perdita dei dati** sarà:
Trascurabile
Il rischio di **Perdita dei dati** si pone dunque nell'area *TRASCURABILE*

In grafica, avremo una immagine come nell'esempio seguente, in cui i punti blu rappresentano i valori del Rischio residuo (Rr).

[6] Cfr. All. 4.2

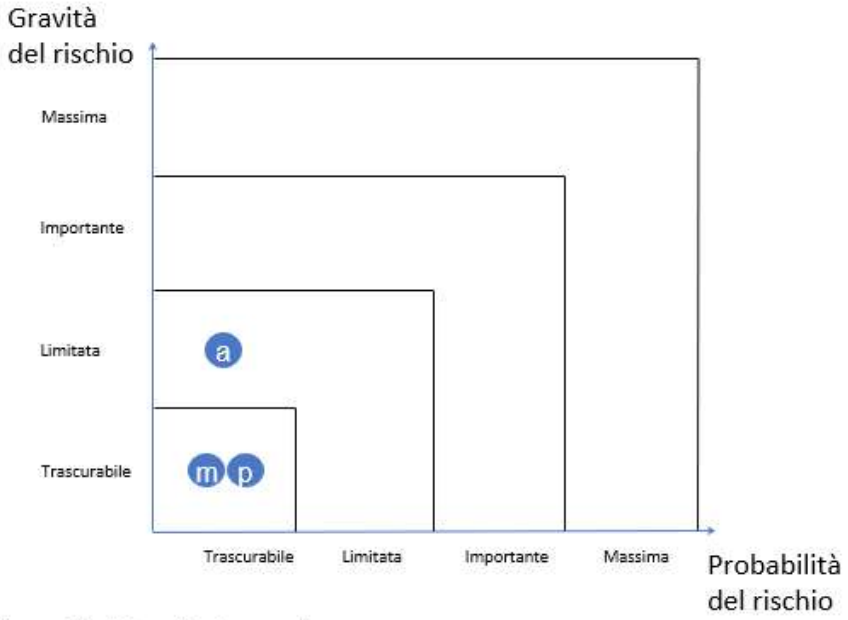


Grafico della valutazione del Rischio residuo (Rr)
ossia il rischio dopo dell'attuazione del Piano di Azione (finalizzato al miglioramento di alcune misure di sicurezza)

a = Accesso illegittimo ai dati personali

m = Modifiche indesiderate ai dati personali

p = Perdita di dati personali

(TABELLA DI ESEMPIO)

L'intero processo di mitigazione potrà essere illustrato graficamente come nell'esempio seguente.

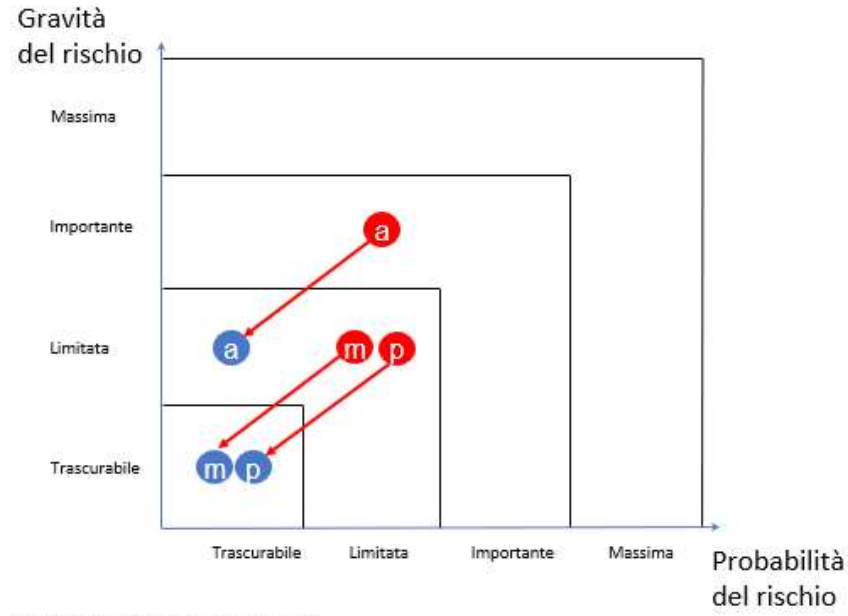


Grafico del processo di mitigazione
ossia il rischio prima e dopo dell'attuazione del Piano di Azione (finalizzato al miglioramento di alcune misure di sicurezza)

a = Accesso illegittimo ai dati personali

m = Modifiche indesiderate ai dati personali

p = Perdita di dati personali

(TABELLA DI ESEMPIO)

2.7 FASE 5 – PARERE DEL DPO/CONSULTAZIONE DEGLI INTERESSATI

2.7.1 PARERE DEL DPO

Ai sensi dell'art. 35, par. 2, GDPR, il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il Responsabile Protezione Dati, qualora ne sia designato uno.
Come accennato (v. punto 2.2) il Gruppo di lavoro WP29, nelle sue Linee guida sui responsabili della protezione dei dati (WP243.rev 01), ha raccomandato che il titolare del trattamento si consulti con il Responsabile Protezione Dati (DPO) per una serie di opinioni, e, in particolare, sulla correttezza della conduzione della DPIA, e sulla conformità al GDPR delle conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare).
Senonché, mediante parere formale, prima della validazione della DPIA, il DPO attesta la conformità della valutazione di impatto alla normativa vigente[7].

2.7.2 CONSULTAZIONE DEGLI INTERESSATI

Qualora lo ritenga necessario, il Titolare deve raccogliere anche le opinioni degli interessati o dei loro rappresentanti (articolo 35, paragrafo 9, GDPR), documentando la propria scelta in apposito documento di accountability allegato alla DPIA.
Nelle Linee Guida Wp248/17 è affermato che "tali opinioni possono essere raccolte attraverso una varietà di mezzi, a seconda del contesto (ad esempio uno studio generico relativo alla finalità e ai mezzi del trattamento, una domanda posta ai rappresentanti del personale oppure indagini abituali inviate ai futuri clienti del Titolare del trattamento)".
Il Titolare valuterà quali siano le modalità più opportune per lo svolgimento della consultazione, tenendo conto che ogni ulteriore trattamento di dati deve essere sorretto da idonea base giuridica.

2.8 FASE 6 – VALIDAZIONE O CONSULTAZIONE PREVENTIVA DEL GARANTE

In fase di validazione della DPIA, il Titolare del trattamento[8] esprime parere favorevole o non favorevole:

- sul calcolo del rischio inerente (Ri);
- sull'efficacia del Piano di Azione previsto (in particolare sulle azioni correttive);
- sul parere del RPD/DPO;
- sull'eventuale consultazione degli interessati.

Infine, il Titolare, preso atto del Rischio residuo (Rr) calcolato:

- se il Rr **rientra nella soglia di accettabilità** (ossia nelle aree LIMITATA o TRASCURABILE), non sarà necessario procedere alla consultazione preventiva dell'Autorità Garante e il trattamento potrà essere *iniziato / continuato*, con opportuni follow-up a cadenza periodica o tutte le volte che ciò si renda necessario (ad esempio in caso di data breach, modifiche rispetto alle informazioni originariamente comunicate, variazioni del rischio rappresentato dalle attività relative al trattamento, indicazioni del RPD/DPO, ecc.);
- se invece il Rr **non rientra nella soglia di accettabilità** (ossia nelle aree IMPORTANTE o MASSIMA, sarà necessario procedere alla consultazione preventiva dell'Autorità Garante per la protezione dei dati personali, ai sensi

[7] Cfr. All. 5.
[8] Cfr. All. 6.

dell'art. 36, GDPR, e del Considerando 94, pertanto, il Titolare dispone che venga comunicata all'Autorità Garante la DPIA svolta nonché i dati di contatto del RPD/DPO, al fine di dare la possibilità all'Autorità di indicare al Titolare le ulteriori misure necessarie per ridurre il livello del rischio ad una soglia di accettabilità.

L'Autorità Garante non avrà il compito di "autorizzare" il trattamento, bensì dovrà indicare al Titolare le ulteriori misure necessarie al fine di ridurre il livello del rischio ad una soglia di accettabilità e potrà, ove necessario, esercitare tutti i poteri attribuitigli dall'art. 58, GDPR: dall'ammonimento fino alla limitazione o al divieto di procedere al trattamento stesso.

Ove con il Parere del Garante, anche nell'esercizio dei poteri di cui all'art. 58, GDPR, si limiti a indicare le misure correttive da adottare, il Titolare del trattamento individua le responsabilità per l'implementazione di tali misure e verifica che il trattamento abbia effettivamente inizio e/o riprenda solo dopo la completa adozione delle stesse.

Il Garante può anche prescrivere eventuali modifiche al trattamento, assicurandosi che lo stesso non sia avviato o continuato se non in conformità alle prescrizioni impartite.

Ove il Garante, nell'esercizio dei poteri di cui all'art. 58, GDPR, imponga la limitazione provvisoria o definitiva del trattamento, il Titolare del trattamento dovrà conformarsi a tale decisione e non procedere all'attività di trattamento.

2.9 AGGIORNAMENTO PERIODICO /OSSERVAZIONI

La DPIA deve essere sottoposta ad osservazione continua nonché aggiornata periodicamente o tutte le volte che ciò si renda necessario.

Tutte le nuove attività devono essere documentate[9].

Tali adempimenti spettano a chi cura le prime fasi della DPIA.

Le osservazioni e gli aggiornamenti periodici devono essere comunicati al DPO e ai vertici aziendali.

Nelle Linee Guida WP248, si suggerisce ai Titolari del trattamento di indicare nel Registro ex art. 30, GDPR, i valori globali di probabilità e di gravità, nonché il valore complessivo del rischio individuato per ciascun trattamento, unitamente alla data di effettuazione dell'ultima valutazione.

La documentazione attestante la conduzione della DPIA e i parametri tenuti in considerazione viene conservata, ai fini di accountability, dal Titolare del trattamento e può essere diffusa soltanto una sintesi della medesima DPIA, concordandone il contenuto con il DPO.

[9] Cfr. All. 7.

Allegato 1

VALUTAZIONE DI IMPATTO PRIVACY (DATA PROTECTION IMPACT ASSESSMENT – DPIA)

Trattamento in valutazione
Es. Pubblicazione on line di documenti amministrativi
ID registro dei trattamenti
Es. RR94

Fase 1 - Valutazione applicazione principi fondamentali

Autore
Es. Soggetto Delegato dell'U.O. di riferimento (Direttore di Struttura) con il supporto del membro del Gruppo di lavoro Privacy competente.
Data
Es. 15/03/2024

Trattamento in considerazione

Descrivere il trattamento, le sue principali caratteristiche e l'eventuale processo nell'ambito del quale si inserisce.

Responsabilità connesse al trattamento

Descrivere i soggetti coinvolti nel trattamento, definendone ruoli e responsabilità situazioni di titolarità o con titolarità, eventuali Responsabili nominati ai sensi dell'art. 28 GDPR, soggetti Delegati/Autorizzati che hanno accesso ai dati.
Es. L'ASL è il Titolare del trattamento dei dati personali.
Il Titolare:
a) definisce le linee organizzative per l'applicazione della normativa di settore;
b) effettua, quando previste, le notificazioni al Garante per la protezione dei dati personali, attraverso i vertici apicali dell'organizzazione amministrativa dell'Azienda;
c) nomina "Responsabile del trattamento" dei dati personali, ove necessario, la società affidataria della gestione e della manutenzione del servizio;
d) detta le linee guida di carattere fisico, logistico ed organizzativo per la sicurezza del trattamento dei dati personali acquisiti;
e) vigila sull'osservanza delle disposizioni impartite;
f) cura gli adempimenti relativi alla protezione dei dati personali, quali l'aggiornamento del registro dei trattamenti, la valutazione di impatto privacy sui diritti e le libertà degli interessati (DPIA), l'attuazione delle misure di sicurezza adeguate al rischio del trattamento.
I dati sono trattati da parte del personale del Titolare, previamente autorizzato ai sensi degli artt. 4.10, 29, 32.4, GDPR e art. 2-quaterdecies del Codice in materia di protezione dati personali, da parte dei soggetti esterni che trattano dati come Titolari autonomi o Contitolari del trattamento.
I fornitori eventualmente nominati quali "Responsabile del trattamento" hanno l'obbligo di attenersi a quanto previsto dalla normativa vigente in tema di trattamento dei dati personali, ivi incluso il profilo della sicurezza, alle disposizioni del presente Regolamento, e alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni previste dalla normativa vigente sulla privacy e delle proprie istruzioni.
Il Responsabile del trattamento impartisce idonee istruzioni atte ad evitare assunzioni o rilevamento non autorizzato di dati da parte delle persone abilitate all'accesso per la manutenzione e riparazione degli impianti.

Standard applicabili al trattamento

Es. *Fonti Normative:*
- Regolamento UE n. 2016/679 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;
- D.Lgs. 30 giugno 2003, n, 196, recante: "Codice in materia di protezione dei dati personali" e successive modificazioni;
- inserire eventuali normative di settore…
-…

Categorie di dati trattati

Es. Nell'ambito delle finalità esplicite, determinate e legitime, il Titolare tratta:
- dati comuni quali dati anagrafici e di contatto, …
- dati relativi alla salute…
- dati genetici…

Ciclo di vita del trattamento dei dati

Descrivere il ciclo di vita dei dati dalla raccolta alla cancellazione o archiviazione.

Risorse di supporto ai dati

Descrivere le risorse di supporto ai dati, fisiche o elettroniche

Eventuali destinatari dei dati (con specifico riferimento ad eventuali Titolari Autonomi)

Es. La comunicazione dei dati personali è possibile in favore di altri soggetti qualificati (ad es. altre autorità pubbliche) cui la comunicazione è dovuta in forza di disposizioni di legge.
I dati personali possono essere oggetto di comunicazione in caso di richieste degli interessati e nell'ambito delle procedure di trasparenza cui il Titolare del trattamento è soggetto (quali ad esempio diritto di accesso documentale ecc.).

Scopi del trattamento e basi giuridiche

Indicare se le finalità del trattamento sono determinate, esplicite e legittime (art. 5, par. 1, lett. b) GDPR).
Es. Le finalità del trattamento dei dati personali (determinate, esplicite e legittime (articolo 5, par. 1, lett. b), GDPR) sono:
….
Per ciascuna finalità, in modo granulare, indicare le basi giuridiche che rendono lecito il trattamento (artt. 6, 9 e 10 GDPR).
Es. La base giuridica del trattamento è costituita dalla necessità di eseguire "un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento", ai sensi dell'art. 6, par. 1, lett. e), GDPR.
Oppure obbligo legale, ecc.
Per il trattamento di categorie particolari di dati personali, la base giuridica è:
es. art. 9, par. 2, lett. g), GDPR ….

Adeguatezza, pertinenza e limitatezza dei dati raccolti.

Indicare in che modo è rispettato il principio di minimizzazione, in relazione alle finalità per cui i dati sono trattati. A tal fine si presti attenzione a: quantità di dati raccolti, tipologia, necessità rispetto agli obiettivi del trattamento (art. 5, par. 1, lett. c) GDPR).
Es. I dati personali oggetto di trattamento vengono:
a) trattati in modo lecito e secondo correttezza per le finalità richiamate;
b) raccolti e registrati per le finalità consentite e resi utilizzabili in altre operazioni di trattamento a condizione che si tratti di attività non incompatibili con tali scopi;

c) raccolti in modo pertinente, completo e non eccedente, rispetto alle finalità per le quali sono raccolti o successivamente trattati.
…

Esattezza e aggiornamento dei dati.

Indicare se i dati sono esatti e aggiornati nonché le misure adottate a tal fine.
Es. I dati sono trattati nel rispetto dei principi di esattezza e aggiornamento.

Tempi di conservazione.

Indicare la data retention per ciascuna finalità nonché i motivi per cui si ritiene che tale periodo sia necessario al raggiungimento delle specifiche finalità indicate (art. 5, par. 1, lett. e) GDPR).
Es. *I dati personali oggetto di trattamento vengono conservati, come imposto dall'art. 5, par. 1, lett. c) ed e), GDPR, per…*

Esercizio dei diritti degli interessati

Indicare come vengono garantiti i diritti degli interessati.
Es. Il Titolare, nel rispetto del principio di correttezza e trasparenza, fornisce informativa agli interessati ai sensi degli aricoli 13 e 14, GDPR….
Gli Interessati possono altresì esercitare i propri diritti, riconosciuti dagli articoli 15-22 del GDPR, come da procedura adottata dall'Ente.
In particolare:

- *con riferimento al diritto di accesso: ….*
- *con riferimento ai diritti di portabilità, di rettifica e di cancellazione dei dati: ….*
- *con riferimento ai diritti di limitazione: …*
- *con riferimento al diritto di opposizione: ….*
- *…*

I diritti di cui al presente articolo riferiti a dati personali concernenti persone decedute possono essere esercitati dagli eredi, da chi abbia un interesse proprio, da chi agisca a tutela dell'interessato o per ragioni familiari considerate particolarmente meritevoli di protezione.
Nell'esercizio dei diritti l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da persona di fiducia.
Nel caso di esito negativo alle istanze, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Rapporti con i responsabili del trattamento

Indicare come vengono disciplinati i rapporti con i responsabili del trattamento.
Es. I rapporti con i Responsabili del trattamento devono essere disciplinati dalla nomina ex art. 28, GDPR, o CCT sul modello emanato dalla Commissione UE nel 2021.
Tale aspetto deve essere verificato con esattezza.

Garanzie riguardanti trasferimenti di dati al di fuori dell'UE o a organizzazioni internazionali

Es. Non sono previsti trasferimenti di dati al di fuori dell'UE o a organizzazioni internazionali.
Oppure: le garanzie riguardanti trasferimenti di dati al di fuori dell'UE o a organizzazioni internazionali siano soddisfatte (capo V GDPR)

Sintesi della valutazione

Es. I principi fondamentali appaiono soddisfatti, tuttavia, appare necessario procedere alla verifica puntuale dell'applicazione del principio informativo e, nell'ambito della definizione di ruoli e responsabilità nel trattamento, della stipula, con la società affidataria del Servizio, della nomina ex art. 28, GDPR, o CCT sul modello emanato dalla Commissione UE nel 2021.

PRINCIPIO	N	M	A
PF1 - Finalità e basi giuridiche del trattamento			X
PF2 - Adeguatezza, pertinenza, limitatezza dei dati			X
PF3 - Esattezza e aggiornamento dei dati			X
PF4 - Periodo di conservazione dei dati			X
PF5 - Informativa ed eventuale raccolta del consenso		X	
PF6 - Diritti degli interessati			X
PF7 - Responsabili del trattamento		X	
PF8 - Trasferimenti di dati personali al di fuori dell'UE			X

Allegato 2

VALUTAZIONE DI IMPATTO PRIVACY (DATA PROTECTION IMPACT ASSESSMENT – DPIA)

Trattamento in valutazione
Es. Pubblicazione on line di documenti amministrativi
ID registro dei trattamenti
Es. RR94

Fase 2 - Misure di sicurezza

Autore
Es. Ufficio Privacy

Data
Es. 30/03/2024

La DPIA procede con l'acquisizione, da parte dell'UP, delle misure di sicurezza tecniche e organizzative esistenti presso l'Azienda per il trattamento sottoposto a valutazione di impatto.
Per le attività di trattamento effettuate per il tramite di un Responsabile del trattamento ai sensi dell'art. 28 GDPR, l'Ufficio privacy ha acquisito le misure di sicurezza del Responsabile dalla nomina o CCT stipulate in precedenza oppure ha richiesto formalmente al Responsabile di riferire sullo stato attuale delle misure.
Conseguentemente, l'UP ha provveduto a compilare la tabella seguente, in cui è riportata anche la valutazione delle singole misure di sicurezza.

Legenda:
Non accettabile (N – colore rosso)
Migliorabile (M – colore giallo)
Accettabile (A - colore verde)
Non Applicabile al trattamento (N/A – colore bianco).

ID	MISURA	DESCRIZIONE	VALUTAZIONE
MS1	**Politiche di tutela della privacy**	*Il Titolare del trattamento ha:* *□ nominato un Responsabile della Protezione dei dati (RPD)* *□ adottato le seguenti procedure:* *a) procedura gestione richieste di esercizio dei diritti degli interessati* *b) procedura gestione data breach* *c) procedura analisi del rischio* *d) procedura DPIA* *e) procedura dismissione apparecchiature elettoniche* *□ provveduto a una ripartizione di compiti e responsabilità "data protection" nominando "Referenti privacy", soggetti "Designati" e i soggetti "Autorizzati" con atto scritto;* *□ censito i dati trattati mediante un Registro dei trattamenti adottato ai sensi dell'art. 30, Reg. UE 2016/679;* *□ apposto un cartello nelle aree videosorvegliate;* *□ fornito agli interessati una informativa sulla protezione dei dati personali che individua il contenuto tassativamente previsto dall'art. 13, par. 1, Reg. UE 2016/679;* *□ elaborato un registro degli accessi alle riprese e una nomina ad hoc ai soggetti autorizzati alla visione delle immagini di videosorveglianza.*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS2	**Gestione del "rischio privacy" specifico per gli Interessati**	*□ Sono state svolte l'analisi dei rischi del trattamento e/o la valutazione di impatto privacy - DPIA.*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS3	**Politiche di cybersecurity e analisi delle vulnerabilità**	*□ Sono state adottate politiche di cybersecurity quali misure di informatica interna e di gestione e governance della sicurezza informatica.* *□ Sono svolte periodiche analisi delle vulnerabilità.* *□ Sono svolti specifici controlli in base a bollettini riservati dello CSIRT o della Polizia postale.*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS4	**Gestione del**	*□ I Dipendenti sono nominati soggetti autorizzati e istruiti*	

	personale (formazione, ruoli e responsabilità, gestione di eventi imprevisti)	*mediante Disciplinare relativo a uso delle postazioni, pc, Internet, posta elettronica, utilizzo supporti removibili e documentazione cartacea; riutilizzo sicuro e dismissione di dispositivi elettronici e supporti; tutela della privacy.* *□ Sono state pianificate misure di sensibilizzazione e formazione del personale sulla cultura della protezione dati e sui principi fondamentali di liceità correttezza e trasparenza, limitazione finalità, minimizzazione, limitazione della conservazione;* *□ Sono adottate misure da adottare una volta cessato il rapporto di lavoro con i soggetti che accedono ai dati.* *□ Formazione specifica al personale sulle vulnerabilità informatiche (furti identità, ransomware, phishing, ecc.).*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS5	**Gestione relazione con le terze parti (formalizzazione incarichi, istruzioni ai Responsabili) che accedono ai dati**	*□ Sono in atto procedure per controllare se gli obblighi dei responsabili del trattamento sono stati definiti con chiarezza e disciplinati da un contratto con clausole che delimitano l'ambito delle rispettive responsabilità (art. 28, GDPR). Nell'ambito dei rapporti con i Responsabili del trattamento, nominati ai sensi dell'art. 28, GDPR, con atto formale, è prevista una procedura volta a ridurre i potenziali rischi per le libertà e la vita privata degli interessati conseguenti all'accesso legittimo ai dati da parte di terzi.* *□ Nella fase di selezione dei Fornitori, essi vengono scelti sulla base di criteri di affidabilità ed è necessario acquisire report/certificazioni sulla sicurezza.* *□ Nel trattamento in analisi, la nomina del fornitore è stata stipulata.* *□ Se è stata stipulata, essa contiene almeno i requisiti di cui all'art. 28, GDPR (in particolare: oggetto, durata, finalità del trattamento e obblighi delle parti; requisiti minimi di autenticazione degli utenti; clausole in materia di restituzione e/o distruzione dei dati allo scadere del contratto; regole per la gestione e la notifica di eventuali incidenti (comunicazione immediata al Titolare del trattamento qualora la violazione riguardi dati personali), nonché un Allegato Tecnico che comprende misure tecniche e organizzative.*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS6	**Vigilanza (audit di conformità)**	*□ Vengono effettuati audit interni periodici, in ogni caso è in adozione una procedura per lo svolgimento di audit di conformità (interni ed esterni) che consentano una visione globale e aggiornata dello stato di protezione dei dati e della conformità con il GDPR (verifica della conformità dei trattamenti, obiettivi e indicatori, responsabilità, ecc.), allo scopo di condurre verifiche ispettive interne ed esterne (a Fornitori) sul campo, nonché adottare e documentare misure (audit di sicurezza, visite agli impianti, ecc.) che consentano di assicurare l'effettività delle garanzie offerte dal responsabile del trattamento in materia di protezione dei dati.*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS7	**Prevenzione da danni fisici e fonti di rischio non umane**	*□ È attivo …… (indicare se vi sono sistemi di sicurezza quali impianti e compartimentazione antincendio, allarmi temperatura e sistemi di rilevazione e auto-spegnimento incendi, gas inerte e interruzione automatica alimentazione; sistema antincendio e idonee procedure per il loro controllo e manutenzione; allarmi anti umidità e antiallagamento sotto pavimento flottante; Impianti di condizionamento e ventilazione; filtri*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL

		antipolvere e altri sistemi di pulizia; derattizzazione, ove necessario, ecc.).	TRATTAMENTO
MS8	**Antiintrusione e controllo degli accessi fisici**	□ *È presente un sistema di controllo degli accessi fisici da parte di dipendenti / fornitori / manutentori/ visitatori / ospiti / utenti ai locali che ospitano il trattamento (indicare quale).* □ *L'attuale sistema di gestione degli accessi controlla l'accesso dei dipendenti dell'ente e dei visitatori esterni.*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS9	**Lotta contro il malware**	□ *Su tutti i pc sono installati antivirus e antimalware, firewall di rete.* □ *Viene svolto un controllo periodico degli aggiornamenti, anche del Sistema Operativo.* □ *Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale dove sono stabilmente archiviati.* □ *è monitorato l'uso e i tentativi di utilizzo di dispositivi esterni.* □ *sono abilitate funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confi-namento, etc. disponibili nel software di base.*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS10	**Sicurezza dei siti web**	□ *Il server del sito web aziendale risiede in UE e ha le misure di sicurezza previste dalla normativa vigente.* □ *Utilizzo di soluzioni provenienti da fornitori affidabili.* □ *Controlli periodici della sicurezza (site-check).* □ *Crittografia del sito con un certificato "Secure Socket Layer" (SSL) e utilizzo del linguaggio di markup HTTPS, che permettono trasferimenti di dati in sicurezza.* □ *Possibilità, per gli utenti, di attivare l'autenticazione a due fattori (anche per le caselle di posta elettronica), laddove ciò sia possibile*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS11	**Sicurezza di server, reti, Wi-Fi**	□ *Gestione dei server e degli apparati di rete.* □ *La policy dell'Ente vieta hotspot con smartphone personali.* □ *Protocolli di comunicazione sicuri basati sull'utilizzo di standard crittografici per la trasmissione elettronica dei dati* □ *Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione è crittografata tramite idonei protocolli (TLS / SSL)* □ *Aggiornamento di firmware, sistemi operativi e software presenti sui server, dispositivi client, componenti attivi della rete, nonché tutti gli ulteriori dispositivi che operano sulla stessa linea di rete* □ *Progettazione e organizzazione dei sistemi informatici in modo tale da segmentare e isolare i sistemi e le reti contenenti i dati, al fine di evitare che il malware si propaghi all'interno delle strutture o verso sistemi esterni all'organizzazione* □ *Installazione di software anti-malware, firewall e sistema di detenzione e prevenzione delle intrusioni* □ *I sistemi di cablaggio rete e gli Impianti di comunicazione wireless sono certificati.* □ *Gestione dei server, degli apparati di rete e del Wi-Fi* □ *Previsione di connessioni WIFI separate per uso interno e per gli ospiti.* □ *Firewall perimetrali che svolgono il ruolo di controller.* □ *Penetration test periodici*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO

MS12	**Sicurezza di hardware, postazioni e dispositivi**	□ *Firewall e antivirus installati su ogni dispositivo* □ *Gli utenti non hanno privilegi per installare o disattivare applicazioni software senza autorizzazione.* □ *Il sistema attiva il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.* □ *È stato effettuato un inventario dei dispositivi autorizzati e non autorizzati.* □ *Le procedure di smaltimento di hardware e altri supporti contenenti dati sono idonee, rendendo impossibile il recupero di dati da supporti dismessi (esempio: è sconsigliato procedere alla dismissione delle stampanti con memoria, senza aver provveduto a cancellare la memoria, poiché un terzo potrebbe acquisire le immagini ottiche degli ultimi documenti stampati o scansionati).* □ *Controllo delle procedure di smaltimento di hardware e altri supporti contenenti dati.* □ *Esistenza di misure adottate per ridurre il rischio che le caratteristiche delle apparecchiature (server, postazioni fisse, portatili, periferiche, dispositivi di comunicazione, supporti rimovibili ecc.) siano utilizzate per danneggiare i dati personali (inventario, compartimentalizzazione, ridondanza, limiti per l'accesso ecc.).* □ *È implementato un sistema di hardware monitoring (con allarmi per surriscaldamenti, guasti componenti, ecc.).* □ *Esportazione dei dati consentita solo agli operatori autorizzati con log delle operazioni di esportazione.* □ *Dispositivi di videosorveglianza (telecamere, dispositivi di rete) protetti da password.* □ *Sistemi di archiviazione delle immagini di proprietà del Titolare gestiti attraverso le policy di sicurezza del Dominio TVCC dedicato.*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS13	**Sicurezza dei software**	□ *Esiste un inventario dei software autorizzati.* □ *Sono programmati dei check su: aggiornamenti periodici dei software, scaricamento di patch di sicurezza, rilevazione di problemi di funzionamento, rilascio di guide per l'utilizzo e divieto di utilizzo per scopi personali.* □ *Rilascio di guide aggiornate e attività di formazione con le nuove versioni che introducono modifiche significative.*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS14	**Manutenzione**	□ *Prevenzione di malfunzionamenti e problemi tecnici dei sistemi.* □ *Esistenza di una politica di manutenzione fisica dei dispositivi, specificando l'eventuale ricorso all'outsourcing, compresa la manutenzione remota, ove autorizzata, con specifica attenzione ai metodi di gestione dei materiali difettosi.* □*Manutenzione interna periodica di Sistemi e di reti (Backup configurazioni, verifica firmware, prestazioni hardware, capienza dischi, utilizzo risorse, ecc.)* □ *Contratti di manutenzione e assistenza hardware e software attivi.* □ *Possibilità di effettuare manutenzioni pianificate senza impatti negativi sulla gestione della funzionalità.* □ *Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS15	**Backup e Restore**	□ *Misure idonee a ripristinare immediatamente la disponibilità e l'accesso dei dati personali in caso di*	

		incidente fisico o tecnico e politiche di backup tali da assicurare la disponibilità e/o l'integrità dei dati personali, tutelandone la confidenzialità (periodicità dei backup, cifratura del canale di trasmissione dati, test di integrità, ecc.) □ *Procedura di backup aggiornata, sicura e testata, con separazione tra i dispositivi utilizzati per i backup a lungo termine e quelli a medio termine, oltre che rispetto a terze parti* □ *Procedure di backup e ripristino dei dati definite, documentate e chiaramente collegate a ruoli e responsabilità* □ *Backup completi eseguiti regolarmente* □ *Monitoraggio dell'esecuzione dei backup per garantirne la completezza* □ *Copie del backup conservate in modo sicuro in luoghi diversi.*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS16	**Business continuity**	□ *è presente un gruppo di continuità, 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).* □ *Tutti i componenti fisici hanno caratteristiche di ridondanza in modo da garantire la Business Continuity. Le macchine virtuali sono configurate in modo da poter ripartire automaticamente su un nodo fisico differente.*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS17	**Disaster recovery**	□ *Disaster Recovery Plan (DRP) contenente l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi, a fronte di gravi emergenze che ne intacchino la regolare attività.* □ *Requisiti per la sicurezza delle informazioni e per la continuità della gestione della sicurezza delle informazioni in seguito a eventi disastrosi.* □ *Sistema per ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi, a fronte di gravi emergenze che ne intacchino la regolare attività (es. terremoti, alluvioni, incendi, ecc.).* □ *Tutti i sistemi sono sotto backup effettuati giornalmente. Il backup viene effettuato su più livelli fisici con storicizzazione fuori linea su nastro. Vengono effettuate prove di restore in modo che sia garantita la possibilità di ripristinare i dati.*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO

MS18	**Controllo degli accessi logici, autenticazione e password**	□ *Esistenza di un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT.* □ *Sono applicate regole per le password.* □ *In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo, l'Ente ha previsto una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e strumenti.* □ *Gli accessi remoti tramite VPN sono gestisti dai firewall perimetrali che si interfacciano direttamente all'active directory, ereditandone quindi tutte le regole di scadenza e complessità definite.* □ *è implementata Autenticazione MFA (multi factor authentication), in particolare per accessi VPN.* □ *Procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati ai soggetti autorizzati al trattamento* □ *Abilitazione all'accesso alla piattaforma di videosorveglianza ai soggetti autorizzati dal Titolare, secondo le specifiche policy di accesso definite ed aggiornate dal Titolare e configurate a livello di Dominio e di piattaforma SW TVCC.* □ *Sono tracciate nei log l'aggiunta o la soppressione di un'utenza amministrativa. Si ha un'allerta quando viene aggiunta un'utenza amministrativa o quando vengano aumentati i diritti di un'utenza amministrativa.*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS19	**Gestione dei profili di accesso**	□ *Definizione dei profili di autorizzazione nei sistemi, separando le attività e le aree di responsabilità per limitare l'accesso degli utenti ai soli dati strettamente necessari per portare a termine i rispettivi compiti.* □ *Gli Utenti interni registrati su dominio accedono ai servizi di rete solo a seguito di autenticazione positiva. Eventuali errori di autenticazione vengono registrati nel Log di sistema e possono essere identificabili attraverso l'Event Viewer di uno dei Domain controller.* □ *Sui vari sistemi (CLIENT, Server, DC) sono state implementate politiche di gestione di Audit che riguardano gli accessi a gruppi di appartenenza, accesso alle cartelle condivise, accesso agli applicativi integrati con AD.* □ *Gli utenti amministratori sono nominativi ed utilizzati solo in caso di effettiva necessità.* □ *Abilitazione all'accesso alla piattaforma di videosorveglianza ai soggetti autorizzati dal Titolare, secondo le specifiche policy di accesso definite ed aggiornate dal Titolare e configurate a livello di Dominio e di piattaforma SW TVCC.*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS20	**Tracciabilità (Logging) degli eventi**	□ *È attivo un servizio di LOG MANAGEMENT degli accessi (login, logout, tentativi falliti) degli Amministratori di Sistema.* □ *Attività degli Amministratori di Sistema registrate tramite log conservati nel rispetto del Provv. Garante 2008.* □ *I dati sono raccolti da uno specifico agent sui DOMAIN CONTROLLER ACTIVE DIRECTORY e inviati ad un sistema di raccolta esterno su CLOUD.* □ *L'agent è anche installato su specifici server ad alto impatto (ad esempio FILE SERVER) per tenere traccia di*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO

		eventuali accessi straordinari fatti con autenticazione locale. □ *I dati dei log sono conservati 6 mesi e sono crittografati.* □ *È attivo un sistema di raccolta e analisi dei log dei firewall* □ *Logging specifico eseguito sulla piattaforma di videosorveglianza per le attività eseguite dagli utenti TVCC abilitati (accesso, visione live, visione playback, esportazione ecc).*	
MS21	**Minimizzazione dei dati personali**	□ *I dati vengono raccolti in ossequio al principio di minimizzazione.*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS22	**Altre misure applicate ai dati**	□ *Pseudonimizzazione e mascheramento dei dati, laddove applicabile, qualora non sia necessaria l'identificazione diretta del soggetto i cui dati si riferiscono, in modo 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.* □ *Anonimizzazione dei dati.* □ *È implementato un sistema di gestione delle chiavi crittografiche.* □ *Le chiavi private sono adeguatamente protette.* □ *Chiavi di cifratura personali.* □ *Formazione relativa alla cifratura.*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS23	**Archiviazione sicura (nella consegna, sistemazione, consultazione) e dismissione sicura**	□ *Sono implementate politiche di conservazione e gestione di archivi elettronici contenenti dati personali, finalizzate a tutelarne, in particolare, la validità giuridica per tutto il periodo necessario (versamento, conservazione, migrazione, accessibilità, eliminazione, politiche di archiviazione, protezione della confidenzialità, ecc.). I dati che non sono più di utilizzo corrente, ma il cui periodo di conservazione non è ancora terminato, per esempio poiché sono conservati in previsione di eventuali contenziosi, dovrebbero essere archiviati.* □ *Sono implementate procedure per la dismissione sicura delle apparecchiature informatiche a fine vita, al fine di evitare il recupero di informazioni da supporti o media dismessi (principalmente memorie di massa).* □ *I dati sono conservati in archivi protetti da una password nota unicamente ai tecnici incaricati dal Responsabile del trattamento.* □ *I dati inseriti sono soggetti a regole di referenzialità che rendono complessa la modifica non controllata dei dati.* □ *Configurazione retention delle immagini pari a 7 giorni sui sistemi di conservazione di proprietà del Titolare.* □ *Cancellazione automatica delle registrazioni oltre il 7° giorno.*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON APPLICABILE AL TRATTAMENTO
MS24	**Archiviazione sicura dei documenti cartacei e**	□ *Politiche relative ai documenti cartacei contenenti dati personali utilizzati nell'ambito del trattamento, che descrivono come i documenti sono stampati, archiviati, distrutti e condivisi.* □ *Procedure per la dismissione sicura dei fascicoli cartacei a fine vita, al fine di evitare il recupero di*	□ NON ACCETTABILE □ ACCETTABILE □ MIGLIORABILE □ NON

	dismissione sicura	*informazioni da documentazione cartacea abbandonata o dismessa.*	APPLICABILE AL TRATTAMENTO

Per i casi in cui:
- la misura non sia applicata (dunque è valutata come “non accettabile”)
- la misura sia applicata ma può essere migliorata (dunque è valutata come “migliorabile”)
si rende necessario prevedere, nel Piano di Azione (fase successiva “Revisione”), azioni correttive al fine di mitigare il rischio.

SINTESI DELLA VALUTAZIONE

ID	MISURA DI SICUREZZA	N	M	A	N/A
MS1	Politiche di tutela della privacy				
MS2	Gestione del "rischio privacy" (specifico per gli Interessati)				
MS3	Politiche di cybersecurity e analisi delle vulnerabilità				
MS4	Gestione del personale (formazione, ruoli e responsabilità, gestione di eventi imprevisti)				
MS5	Gestione relazione con le terze parti che accedono ai dati				
MS6	Vigilanza (audit di conformità)				
MS7	Prevenzione da danni fisici e fonti di rischio non umane				
MS8	Antiintrusione e controllo degli accessi fisici				
MS9	Lotta contro il malware				
MS10	Sicurezza dei siti web				
MS11	Sicurezza di server, reti, Wi-Fi				
MS12	Sicurezza di hardware, postazioni e dispositivi				
MS13	Sicurezza dei software				
MS14	Manutenzione				
MS15	Backup e Restore				
MS16	Business continuity				
MS17	Disaster recovery				
MS18	Controllo degli accessi logici, autenticazione, password				
MS19	Gestione dei profili di accesso				
MS20	Tracciabilità (Logging) degli eventi e monitoraggio integrità dei dati				
MS21	Minimizzazione dei dati				
MS22	Altre misure applicate ai dati				
MS23	Archiviazione e dismissione sicura (nella consegna, sistemazione, consultazione)				
MS24	Archiviazione e dismissione sicura dei documenti su carta				

Allegato 3

VALUTAZIONE DI IMPATTO PRIVACY (DATA PROTECTION IMPACT ASSESSMENT – DPIA)

Trattamento in valutazione
Es. Pubblicazione on line di documenti amministrativi
ID registro dei trattamenti
Es. RR94

Fase 3 – Valutazione Rischio inerente (Ri)

Autore
Es. Ufficio Privacy

Data
Es. 15/04/2024

Il rischio inerente o potenziale (Ri) è il rischio calcolato prima dell'applicazione delle misure di sicurezza.

Rischio inerente = Probabilità (Minaccia) * Gravità (Impatto)
Ri = P * G

Il risultato corrisponde a una scala di valori: potremo avere un rischio inerente (Ri) trascurabile, limitato, importante, massimo.

La DPIA, dunque, in tale frangente, prevede la "verifica" delle fonti di rischio, della natura e della particolarità dei rischi, delle minacce che possono concretizzare il rischio.
Ciò, per poi passare alla "valutazione" dei rischi per i diritti e le libertà degli interessati, procedendo, in particolare, dalla prospettiva degli interessati mediante una stima di:
- probabilità (P) che si verifichino eventi che potrebbero determinare accesso illegittimo, modifica indesiderata, perdita dei dati, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure esistenti.
- gravità (G) dei rischi, ossia gli impatti potenziali per i diritti e le libertà degli interessati, nei casi di accesso illegittimo, modifica indesiderata, perdita dei dati (facendo riferimento, per gli impatti, alla seguente legenda).

LIVELLO	Impatto fisico	Esempio	Impatto materiale	Esempio	Impatto psicologico	Esempio
Trascurabile	Gli interessati potrebbero incontrare qualche inconveniente fisico, superabile senza difficoltà.	Mal di testa passeggero.	Gli interessati potrebbero incontrare qualche inconveniente materiale, superabile senza difficoltà.	Perdita di tempo dovuta a ripetizione delle procedure o all'attesa della loro effettuazione, riutilizzo dei dati a scopo di pubblicità mirata per beni di consumo corrente.	Gli interessati potrebbero incontrare qualche inconveniente psicologico, superabile senza difficoltà.	Semplice fastidio, impressione di violazione della privacy senza danno reale (intrusione commerciale).
Limitato	Gli interessati potrebbero sperimentare inconvenienti fisici superabili nonostante alcune difficoltà.	Malattia lieve a seguito del mancato rispetto di controindicazioni, diffamazione che dia luogo a rappresaglie fisiche.	Gli interessati potrebbero avere inconvenienti materiali, superabili nonostante alcune difficoltà.	Pagamenti non pianificati (ad esempio multe non dovute), negazione dell'accesso a servizi amministrativi o commerciali, pubblicità online mirata su un aspetto di vita privata che la persona voleva mantenere riservata.	Gli interessati potrebbero avere inconvenienti psicologici, superabili nonostante alcune difficoltà.	Disturbo psicologico minore ma oggettivo, senso di violazione della privacy senza danni irreparabili, intimidazione sui social network.
Importante / Significativo	Gli interessati potrebbero subire conseguenze fisiche significative, che dovrebbero essere in grado di superare, ma con notevoli	Aggravamento dello stato di salute a seguito di una errata assunzione di responsabilità o del mancato rispetto di controindicazioni, alterazione	Gli interessati potrebbero subire conseguenze materiali significative, che dovrebbero essere in grado di superare, ma con notevoli	Perdite monetarie non indennizzate, perdita di opportunità uniche e non ricorrenti (mutui immobiliari, studi, occupazioni, esami scolastici), perdita dell'abitazione, del posto di lavoro.	Gli interessati potrebbero subire conseguenze psicologiche significative, che dovrebbero essere in grado di superare, ma	Grave disturbo psicologico (depressione, fobie), senso di violazione della privacy e di un danno irreparabile, esposizione a ricatti, cyberbullismo e molestie

	difficoltà.	dell'integrità fisica.	difficoltà.		con notevoli difficoltà.	psicologiche.
Massimo	Gli interessati potrebbero sperimentare gravi conseguenze fisiche, anche irrimediabili, che potrebbero non superare.	Affezione fisica a lungo termine o permanente, alterazione permanente dell'integrità fisica, decesso.	Gli interessati potrebbero subire gravi conseguenze materiali, anche irrimediabili, che potrebbero non superare.	Rischio finanziario, indebitamento ingente, impossibilità di lavorare, incapacità di ricollocazione, smarrimento di elementi di prova nell'ambito di un contenzioso, perdita di accesso a infrastrutture vitali (acqua, elettricità, ecc.).	Gli interessati potrebbero subire gravi conseguenze psicologiche, anche irrimediabili, che potrebbero non superare.	Disturbo psicologico a lungo termine, sanzione penale, allontanamento, perdita di legami familiari, perdita capacità di agire, cambio di stato amministrativo e/o perdita dell'autonomia legale (tutela).

La stima del rischio ottenuta è la seguente.

Accesso illegittimo ai dati	
Potenziali impatti sugli interessati se il rischio si dovesse concretizzare.	*Esempio: selezionare impatti da tabella precedente*
Principali minacce che potrebbero concretizzare il rischio.	*Esempio: virus informatico*
Fonti di rischio.	*Esempio: mancato aggiornamento del SO, mancanza di firewall e/o antivirus sul pc, ecc.*
Misure che contribuiscono a mitigare il rischio.	*Esempio: selezionare tra le misure di cui all'Allegato 2*
Stima della gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure esistenti.	*Esempio: IMPORTANTE*
Stima della probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure esistenti.	*Esempio: LIMITATA*
Modifiche indesiderate dei dati	
Potenziali impatti sugli interessati se il rischio si dovesse concretizzare.	*Esempio: selezionare impatti da tabella precedente*
Principali minacce che potrebbero concretizzare il rischio.	*Esempio: errore del soggetto autorizzato nel modificare i dati*
Fonti di rischio.	*Esempio: mancata formazione dei soggetti che intervengono nel trattamento, ecc.*
Misure che contribuiscono a mitigare il rischio.	*Esempio: selezionare tra le misure di cui all'Allegato 2*
Stima della gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure esistenti.	*Esempio: Il rischio è LIMITATA*
Stima della probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure esistenti.	*Esempio: Il rischio è LIMITATA*
Perdita dei dati	
Potenziali impatti sugli interessati se il rischio si	*Esempio: selezionare impatti da tabella*

dovesse concretizzare.	*precedente*
Principali minacce che potrebbero concretizzare il rischio.	*Esempio: ransomware e conseguente impossibilità di utilizzo dei servizi*
Fonti di rischio.	*Esempio: Falla nella sicurezza, mancata formazione dei soggetti che intervengono nel trattamento*
Misure che contribuiscono a mitigare il rischio.	*Esempio: selezionare tra le misure di cui all'Allegato 2*
Stima della gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure esistenti.	*Esempio: Il rischio è LIMITATA*
Stima della probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure esistenti.	*Esempio: Il rischio è LIMITATA*

Tale stima dei valori probabilità (P) e gravità (G) per accesso (a), modifica (m) e perdita (p) dei dati è sintetizzata graficamente nell'immagine seguente, in cui i punti rossi rappresentano i valori del rischio inerente (Rr).

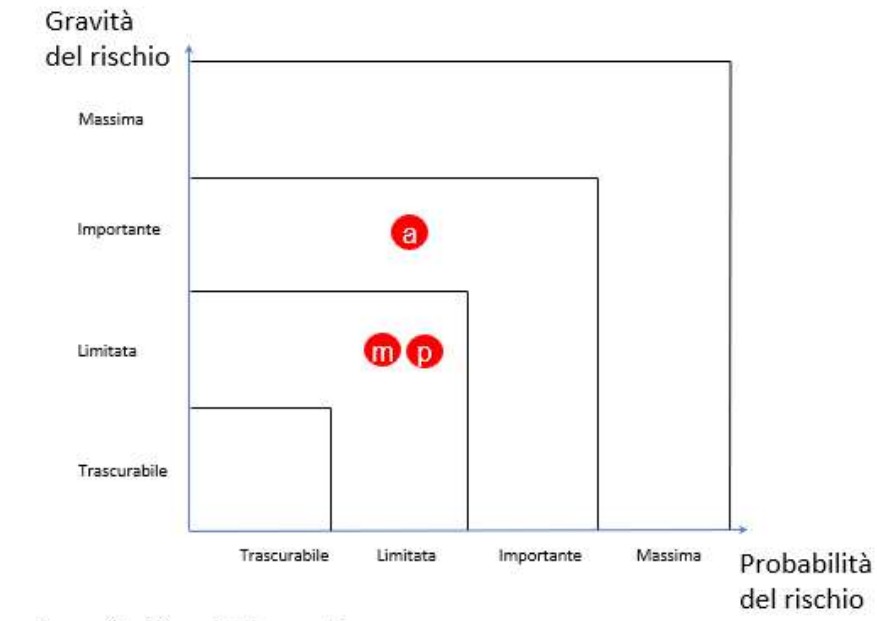


Grafico della valutazione del Rischio Inerente (Ri)
ossia il rischio prima dell'attuazione del Piano di Azione (finalizzato al miglioramento di alcune misure di sicurezza)

(TABELLA DI ESEMPIO)

Allegato 4.1

VALUTAZIONE DI IMPATTO PRIVACY (DATA PROTECTION IMPACT ASSESSMENT – DPIA)

Trattamento in valutazione
Es. Pubblicazione on line di documenti amministrativi
ID registro dei trattamenti
Es. RR94

Fase 4 - Revisione.

Autore
Es. Ufficio Privacy

Data
Es. 30/04/2024

Calcolato il rischio inerente (Ri), laddove lo standard di accettabilità della misura non sia rispettato, è necessario determinare misure aggiuntive finalizzate a mitigare il rischio, come indicato dal regolamento all'art. 35, par. 7, lett. d), e nel Considerando 90.

Per ciascuna misura valutata come MIGLIORABILE o come NON ACCETTABILE, si configurano come necessarie le seguenti azioni correttive.

Piano di azione

ID MISURA	**MISURA AGGIUNTIVA O CORRETTIVA**	**TERMINE**	**SOGGETTO**
MS6	***Vigilanza (audit di conformità)*** • *è necessario adottare una Procedura di audit, interni ed esterni, che consenta di avere una visione globale e aggiornata dello stato di protezione dei dati e della conformità con il GDPR, allo scopo di condurre verifiche ispettive interne ed esterne sul campo, nonché adottare e documentare misure che consentano di assicurare l'effettività delle garanzie offerte dai responsabili del trattamento in materia di protezione dei dati.*	*30/06/2024*	*UP, con il supporto del DPO*
MS13	***Sicurezza dei software*** • *Predisporre un inventario dei software in uso*	*31/08/2024*	*Settore Informatico*

Si da mandato ai soggetti indicati di attuare, entro la tempistica, le misure correttive previste nel Piano di Azione.

Allegato 4.2

VALUTAZIONE DI IMPATTO PRIVACY (DATA PROTECTION IMPACT ASSESSMENT – DPIA)

Trattamento in valutazione
Es. Pubblicazione on line di documenti amministrativi
ID registro dei trattamenti
Es. RR94

Fase 4 - Attuazione del Piano di Azione.

Autore
Es. Ufficio Privacy

Data
Es. 15/09/2024

Mediante il presente documento, si da atto che le azioni correttive previste nel Piano di Azione:

□ sono state attuate integralmente
(*indicare le modalità)*

□ sono state attuate parzialmente
(indicare le modalità)

□ non sono state attuate
(indicare I motivi della mancata attuazione)

Alla luce di quanto sopra, il rischio residuo (Rr) del trattamento per ciascun evento accesso (a), modifica (m) e perdita (p) dei dati, ossia

Rischio residuo = Probabilità (Minaccia) * Gravità (Impatto) / Efficacia (Misure aggiuntive o correttive)

$$Rr = \frac{P * G}{E}$$

è il seguente:

Alla luce del piano d'azione, la **gravità** del rischio di **Accesso illegittimo ai dati** è:
Limitata
Alla luce del piano d'azione, la **probabilità** del rischio di **Accesso illegittimo ai dati** è:
Trascurabile
Il rischio di **Accesso illegittimo ai dati** si pone dunque nell'area *LIMITATA (poiché viene rilevato il valore più grande tra gravità e probabilità)*

Alla luce del piano d'azione, la **gravità** del rischio di **Modifiche indesiderate ai dati** è:
Trascurabile
Alla luce del piano d'azione, la **probabilità** del rischio di **Modifiche indesiderate ai dati** è:
Trascurabile
Il rischio di **Modifiche indesiderate ai dati** si pone dunque nell'area *TRASCURABILE*

Alla luce del piano d'azione, la **gravità** del rischio di **Perdita dei dati** è:
Trascurabile
Alla luce del piano d'azione, la **probabilità** del rischio di **Perdita dei dati** è:
Trascurabile
Il rischio di **Perdita dei dati** si pone dunque nell'area *TRASCURABILE*

Graficamente, i punti blu rappresentano i valori del Rischio residuo (Rr):

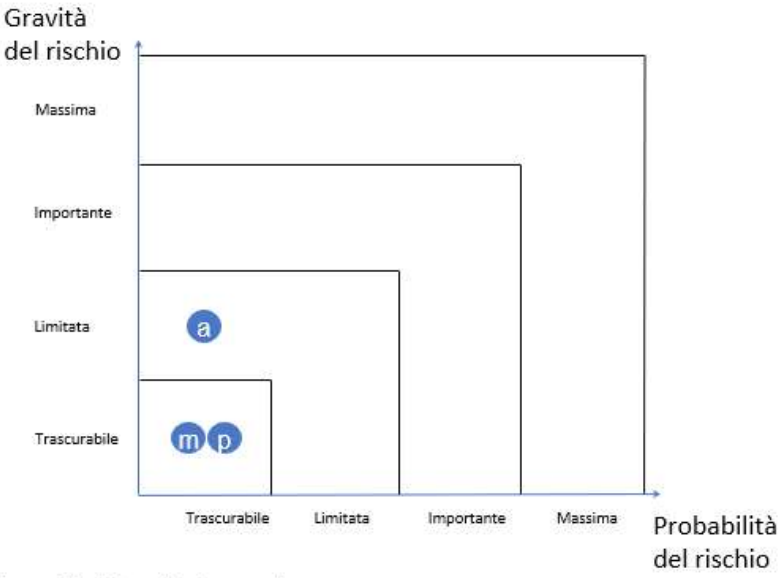


Grafico della valutazione del Rischio residuo (Rr)
ossia il rischio dopo dell'attuazione del Piano di Azione (finalizzato al miglioramento di alcune misure di sicurezza)

a = Accesso illegittimo ai dati personali

m = Modifiche indesiderate ai dati personali

p = Perdita di dati personali

(TABELLA DI ESEMPIO)

L'intero processo di mitigazione è illustrato graficamente nella seguente immagine:

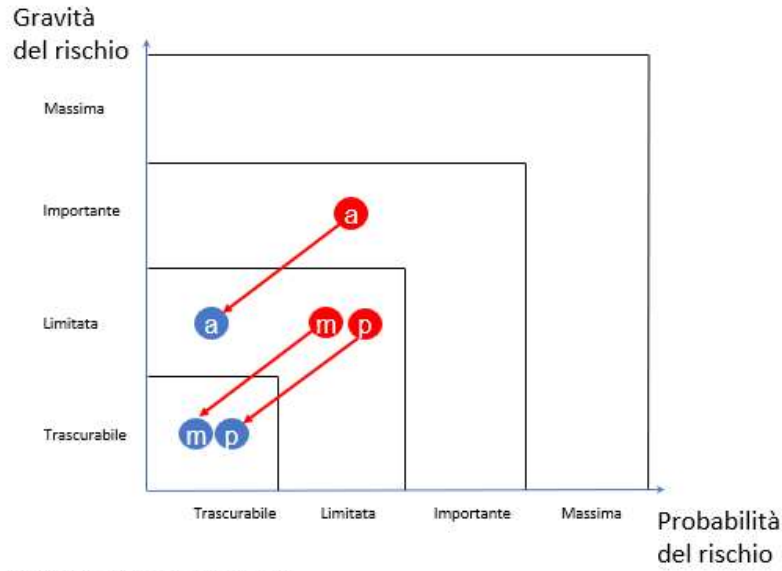


Grafico del processo di mitigazione
ossia il rischio prima e dopo dell'attuazione del Piano di Azione (finalizzato al miglioramento di alcune misure di sicurezza)

a = Accesso illegittimo ai dati personali

m = Modifiche indesiderate ai dati personali

p = Perdita di dati personali

(TABELLA DI ESEMPIO)

Si dispone l'invio della DPIA al RPD/DPO dell'Azienda, con richiesta di parere formale sul corretto svolgimento della DPIA (descrizione sistematica dei trattamenti e delle finalità, necessità e proporzionalità dei trattamenti in relazione alle finalità, valutazione dei rischi per i diritti e le libertà degli interessati, misure previste nel Piano di Azione allo scopo di mitigare i rischi).

Allegato 5

VALUTAZIONE DI IMPATTO PRIVACY (DATA PROTECTION IMPACT ASSESSMENT – DPIA)

Trattamento in valutazione
Es. Pubblicazione on line di documenti amministrativi
ID registro dei trattamenti
Es. RR94

Fase 5 – Parere del DPO sul corretto svolgimento della DPIA.

Autore
DPO

Data
Es. 30/09/2024

ASL TO 4
Ufficio Privacy

OGGETTO: Parere sulla valutazione d'impatto (Data Protection Impact Assessment - DPIA) ai sensi degli artt. 35, par. 2, e 39, par. 1, lett. c), GDPR, relativamente al trattamento ……

Il sottoscritto ……, tel. ……, e-mail ……, PEC ……, nella sua qualità di rappresentante legale della Cap&G s.r.l., Responsabile della Protezione dei dati (RPD/DPO) dell'ASL TO4,

Premesso che

- il Titolare del trattamento, ai sensi dell'art. 5, par. 2, GDPR, è competente per il rispetto delle disposizioni relative alla protezione delle persone fisiche a riguardo del trattamento dei dati personali, ai sensi dell'articolo 35, par. 2, GDPR;
- il Gruppo di lavoro WP29 (Linee guida sui responsabili della protezione dei dati, adottate il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017 - WP243.rev 01) ha raccomandato che il titolare del trattamento richieda al proprio RPD/DPO un parere sulla DPIA svolta
- il Titolare del trattamento ha inviato la DPIA svolta richiedendo un Parere formale;

rilascia il seguente parere sulla valutazione d'impatto privacy (Data Protection Impact Assessment - DPIA) ai sensi degli artt. 35, par. 2, e 39, par. 1, lett. c), GDPR.

Rilevato che

la descrizione sistematica dei trattamenti previsti e delle finalità del trattamento

☐ è adeguata ☐ non è adeguata

la valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità

☐ è adeguata ☐ non è adeguata

la valutazione dei rischi per i diritti e le libertà degli interessati

☐ è adeguata ☐ non è adeguata

le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la adeguatezza al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone

☐ sono adeguate ☐ non sono adeguate

Sulla base dei documenti pervenuti

Vista la normativa vigente in materia di protezione dei dati personali

☐ **attesta**

di non poter esprimere un parere, poiché sono necessari ulteriori approfondimenti istruttori, ed invita il Titolare del Trattamento a integrare l'istanza di parere, astenendosi, nelle more, dal compiere operazioni del trattamento

☐ **esprime parere**

☐ Favorevole *in quanto la DPIA è stata svolta correttamente, le salvaguardie applicate per attenuare i rischi per i diritti e gli interessi delle persone interessate sono efficaci e le sue conclusioni sono conformi al GDPR.*

☐ Non favorevole *in quanto…….*

In ogni caso è necessario che venga svolta una verifica periodica sull'applicazione delle misure di sicurezza, per un aggiornamento continuo della DPIA e ripetizione della procedura ove muti sostanzialmente il trattamento dei dati.

Data e luogo

Il Responsabile della Protezione dei dati

……..

firma

_____

Allegato 6

VALUTAZIONE DI IMPATTO PRIVACY (DATA PROTECTION IMPACT ASSESSMENT – DPIA)

Trattamento in valutazione
Es. Pubblicazione on line di documenti amministrativi
ID registro dei trattamenti
Es. RR94

Fase 6 – Validazione

Autore
Es. Direttore Generale/Direttore Amm.vo/Direttore di S.C.

Data
Es. 15/10/2024

Indicare la natura dell'atto (es. Determinazione Dirigenziale, Deliberazione, ecc.)

OGGETTO: Valutazione d'impatto sulla protezione dati (Data Protection Impact Assessment - DPIA) ai sensi degli artt. 35, par. 2, e 39, par. 1, lett. c), GDPR, relativamente al trattamento ……

Il sottoscritto ……., tel. ……., e-mail ……., PEC ……., nella sua qualità di ……. dell'ASL TO4,

Premesso che

- il Titolare del trattamento dei dati personali, ai sensi dell'art. 5, par. 2, GDPR, è competente per il rispetto delle disposizioni relative alla protezione delle persone fisiche a riguardo del trattamento dei dati personali, ai sensi dell'articolo 35, par. 2, GDPR;
- in data …. l'UP di questa Azienda ha avviato la Valutazione d'impatto sulla protezione dati (Data Protection Impact Assessment - DPIA), che si è svolta regolarmente, nel rispetto della procedura adottata in data ….. con Deliberazione n. …..;
- con nota prot. n. …. del ……., il RPD/DPO di questa Azienda ha rilasciato parere postitivo sulla DPIA svolta;
- si rende necessario un ultimo passaggio di "validazione" della DPIA

Sulla base dei documenti pervenuti e/o degli accertamenti compiuti

Vista la normativa vigente in materia di protezione dei dati personali

esprime parere

☐ Favorevole ☐ Non favorevole

sul calcolo del rischio inerente (Ri)

☐ Favorevole ☐ Non favorevole

sull'efficacia del Piano di Azione previsto (in particolare sulle azioni correttive)

☐ Favorevole ☐ Non favorevole

sul parere del RPD/DPO

☐ **valida il Rischio residuo (Rr)** del trattamento/dei trattamenti sottoposto/i a DPIA **poiché rientra nella soglia di accettabilità (ossia nelle aree LIMITATA o TRASCURABILE)**, dunque non è necessario procedere alla consultazione preventiva dell'Autorità Garante e il trattamento potrà essere *iniziato / continuato*, con opportuni follow-up a cadenza periodica o tutte le volte che ciò si renda necessario (ad esempio in caso di data breach, modifiche rispetto alle informazioni originariamente comunicate, variazioni del rischio rappresentato dalle attività relative al

trattamento, indicazioni del RPD/DPO, ecc.). La documentazione attestante la conduzione della DPIA viene conservata, ai fini di accountability, dall'Ufficio Privacy e non viene pubblicata nella Sezione "Trasparenza" del sito web aziendale.

☐ **non valida il Rischio residuo (Rr)** del trattamento/dei trattamenti sottoposto/i a DPIA **poiché non rientra nella soglia di accettabilità (ossia è nelle aree IMPORTANTE o MASSIMA)**, dunque, è necessario procedere alla consultazione preventiva dell'Autorità Garante per la protezione dei dati personali, ai sensi dell'art. 36, GDPR, e del Considerando 94. In tal senso dispone che:
- venga comunicata all'Autorità Garante la DPIA svolta nonché i dati di contatto del RPD/DPO, al fine di dare la possibilità all'Autorità di indicare al Titolare le ulteriori misure necessarie per ridurre il livello del rischio ad una soglia di accettabilità;
- il trattamento abbia effettivamente inizio e/o riprenda soltanto dopo la completa adozione delle richiamate misure.
Con provvedimento successivo, verranno individuate le responsabilità per l'implementazione delle misure indicate dall'Autorità.

Data e luogo

Firma

_____

N.B. : La documentazione attestante la conduzione della DPIA e i parametri tenuti in considerazione viene conservata, ai fini di accountability, dal Titolare del trattamento e può essere diffusa soltanto una sintesi della medesima DPIA, concordandone il contenuto con il DPO.

Allegato 7

VALUTAZIONE DI IMPATTO PRIVACY (DATA PROTECTION IMPACT ASSESSMENT – DPIA)

Trattamento in valutazione
Es. Pubblicazione on line di documenti amministrativi
ID registro dei trattamenti
Es. RR94

Fase 7 – Aggiornamento periodico / Osservazioni

Autore
Es. Direttore di S.C./UP

Data
Es. 15/10/2025

Comunicazione aggiornamenti

Aggiornamento n. 1 del __/__/____ (prot. N. _____ del _____)

Sono sopravvenute le seguenti modifiche, rispetto alle informazioni originariamente comunicate (indicare in modo specifico circostanze che sono cambiate rispetto a come rappresentate nella originaria richiesta di DPIA: es., mezzi del trattamento, qualità e quantità dei dati, etc.):

_____
_____
_____
_____

Sono subentrate variazioni del rischio rappresentato dalle attività relative al trattamento (indicare se vi sono state modifiche sul rischio originariamente considerato):

_____
_____
_____
_____

Sono stati rilevati i seguenti Data breach:

_____
_____
_____
_____

Altre informazioni:

_____
_____
_____
_____

Osservazione n. 1 del ___/___/_____

Nuove attività rilevate: ……

Data e luogo

Firma

_____

N. B.: Le osservazioni e gli aggiornamenti periodici devono essere comunicati al DPO e ai vertici aziendali.