SPV Linea M4 S.p.A.

PROCEDURA

Data Protection Impact Assessment

edizione 1.

INDICE DEL DOCUMENTO

1. INFORMAZIONI INTRODUTTIVE

Ogni qualvolta sia pianificato un progetto o una iniziativa che possa avere impatto sul trattamento di dati personali devono essere utilizzate le fasi previste nella procedura (privacy by design).
Premesso che il processo di analisi deve essere attivato fin dall'inizio della progettazione e comunque prima di acquisire e trattare dai personali, può capitare che non tutte le informazioni richieste siano immediatamente disponibili. In questo caso si può specificare che una certa informazione non è ancora stata acquisita/valutata. Tuttavia è necessario disporre di tutte le informazioni prima di prendere impegni vincolanti con terze parti (ad esempio fornitori di servizi tecnici per il progetto). Quindi, il momento migliore per utilizzare la check-list è quando il progetto, uscito dalla fase embrionale di prima ideazione entra nel vivo delle valutazioni tecniche di concreta fattibilità.

Di seguito si riportano i casi in cui, ai sensi dell'Art. 35 del Regolamento (UE) 2016/679 del 27 aprile 2016, è necessaria la valutazione d'impatto sulla protezione dei dati (identificato con Data Protection Impact Assessment o DPIA):

- 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.

Le predette casistiche vanno costantemente aggiornate alla luce dei provvedimenti emessi in materia dal Garante per la Protezione dei Dati Personali.

La presente procedura disciplina il processo DPIA di SPV Linea M4 S.p.A. (di seguito anche solo "**M4**" o "**la Società**") a partire dalle analisi del rischio per ogni trattamento di dati personali fino alla fase di valutazione del rischio prima di effettuare tale trattamento.

Qui di seguito si riportano le IV fasi del Processo, dettagliate operativamente nell'**allegato 1 – M4_DPIA-checklist:**

- Fase I – Descrizione del trattamento (privacy by design);
- Fase II – Valutazione di impatto sulla protezione dei dati personali;
- Fase III – Approfondimento della valutazione di impatto sulla protezione dei dati personali;
- Fase IV – Finalizzazione della valutazione di impatto sulla protezione dei dati personali.

1.1 Destinatari

É destinatario della presente procedura il personale di **M4** appartenente a tutte le Funzioni a diverso titolo coinvolte nei processi di trattamenti di dati personali considerati a "rischio".
I principi e le regole della procedura si intendono rivolte anche a soggetti terzi, ad esempio fornitori chiave, in particolare nei casi in cui condividano il trattamento, per quanto ad essi applicabili in virtù dei rapporti in essere con la stessa.

1.2 Principali riferimenti normativi e di Compliance

Riferimenti interni

- Registro del trattamento.

Riferimenti esterni

- GDPR – General Data Protection Regulation;
- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 29);

1.3 Definizioni

Finalità del trattamento	Rappresenta il processo aziendale nell'ambito del quale è necessario effettuare uno o più trattamenti di dati personali.
Scopo/Tipologia del trattamento	Rappresenta la specifica attività aziendale che prevede il trattamento di dati personali. Ai sensi dell'articolo 4 comma 2) per trattamento si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali.
Categoria degli interessati	Categoria di persone fisiche a cui fanno riferimento i dati trattati (es. dipendenti, fornitori, clienti retali, referenti di clienti B2B, prospect, ecc...).
Categorie di dati personali	Categorizzazione della natura dei dati trattati, rientrante in una delle categorie di seguito identificate: • Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (artt. 9 e 10 del GDPR); • Dati personali e identificativi (art. 4 del GDPR); Dati richiamati ai sensi dell'Art. 4 del GDPR e delle Linee Guida WP29: • Dati retributivi, contributivi, assicurativi; • Dati relative alle assenze di breve e lungo periodo; • Dati relativi a provvedimenti disciplinari; • Dati riguardanti le performance lavorative o professionali; • Abitudini di acquisto; • Dati che consentono la geolocalizzazione; • Dati giudiziari; • Altre categorie non elencate in precedenza.
Funzioni aziendali	Direzioni/Funzioni Aziendali che effettuano il trattamento di dati personali della Società.
Soggetti terzi	Soggetti esterni all'organizzazione che effettuano il trattamento di dati personali in nome e per conto della Società. Per i soggetti terzi si richiede la denominazione sociale e la sede legale. Ai sensi dell'articolo 4 comma 9) si intende per destinatario la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati 4.5.2016 L 119/33 Gazzetta ufficiale dell'Unione europea IT membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.
Responsabili esterni del trattamento/ eventuali contitolari	Ai sensi dell'articolo 4 comma 8) per responsabile del trattamento si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Trasferimenti di dati personali verso paesi extra-UE	Ai sensi dell'articolo 4 comma 23) si intende per trattamento transfrontaliero: a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.

Termini ultimi previsti per la cancellazione	Ciascuna prassi aziendale che prevede la cancellazione/distruzione di dati personali o documenti contenetti dati personali al superamento di un determinato arco temporale.
Applicativi/Sistemi	Soluzioni informatiche, applicativi/software, moduli cartacei/digitali, siti internet o dossier utilizzati per il trattamento dei dati.
Documenti cartacei/Database	Moduli cartacei/digitali per il trattamento dei dati.
Misure di sicurezza tecniche organizzative	Indicazione delle misure, specifiche per ciascun processo, che mitigano il rischio di trattamento improprio (es. eccedente rispetto agli obiettivi aziendali o effettuato da persona che non sono incaricate del trattamento) dei dati. A titolo puramente esemplificativo, alcune misure sono ad esempio il blocco delle porte USB, l'accesso vincolato a sistemi utilizzati esclusivamente da specifiche funzioni, procedure riguardanti il trattamento dei dati che prevedono specifiche modalità di catalogazione/archiviazione dei dati.

2. FASE I - DESCRIZIONE DEL TRATTAMENTO (PRIVACY BY DESIGN)

Fase	A cosa serve	Chi	Come	Quando
FASE I Descrivi	Serve a capire se nell'iniziativa sono presenti elementi minimi di rischio da approfondire con una valutazione di impatto ai fini privacy	La Funzione che attiva l'iniziativa, insieme ad IT in caso di utilizzo di piattaforme tecnologiche, con il supporto della Funzione Compliance	A mezzo della checklist di fase I (Privacy by Design)	Ogni qualvolta sia pianificata un'iniziativa o un progetto. Da attivare fin dall'inizio della progettazione
Fase	**A cosa serve**	**Chi**	**Come**	**Quando**
FASE II Valuta	Con gli elementi raccolti in fase I, serve a decidere se attivare o meno una valutazione di impatto	Funzione richiedente + IT + Legal + DPO/Privacy Champion	A mezzo di confronto con il DPO/Privacy Champion e compilazione esito di fase II	Al termine della fase I e comunque prima dell'inizio del trattamento dei dati
Fase	**A cosa serve**	**Chi**	**Come**	**Quando**
FASE III Approfondisci	Serve ad effettuare la valutazione di impatto	Funzione richiedente + IT + Legal	A mezzo checklist della fase III	Prima dell'inizio del trattamento dei dati
Fase	**A cosa serve**	**Chi**	**Come**	**Quando**
FASE IV Finalizza e chiudi la valutazione	Serve a valutare gli esiti della valutazione di impatto e decidere le azioni conseguenti (ad esempio comunicazioni alle autorità)	Funzione richiedente + IT + Legal + DPO/Privacy Champion	A mezzo di confronto con il DPO/Privacy Champion e compilazione esito di fase IV	Prima dell'inizio del trattamento dei dati

A) DESCRIZIONE E AMBITO DEL PROGETTO

La **FASE 1** ha come obiettivo l'individuazione delle peculiarità del progetto oggetto di analisi,

Tale fase è utile alla Società a identificare eventuali rischi da approfondire con una valutazione d'impatto ai fini privacy. La valutazione dei rischi ovviamente deve essere condotta alla luce delle indicazioni metodologiche definite dal Regolamento (Ue) 2016/679 Del Parlamento Europeo E Del Consiglio Del 27 aprile 2016 (di seguito GDPR). A tale scopo è opportuno prevedere una descrizione dei trattamenti previsti e dei relativi elementi di caratterizzazione.
In tale ambito vengono raccolte le seguenti informazioni:

- Scopo del progetto;
- Tecnologia che si intende utilizzare;
- I principali fornitori di servizi;
- Modalità di erogazione del servizio;
- Area geografica di riferimento.

- Il progetto si rivolge a utenti situati in Europa? - Se si specificare quali paesi UE coinvolti.
- Il progetto coinvolge fornitori extra europei o piattaforme tecnologiche extraeuropee? - Se si specificare quali partner non UE coinvolti (ad esempio nel caso in cui si utilizzino servizi in Cloud ospitati su server extra UE).

In tale fase si focalizza l’attenzione sulle modalità di erogazione del servizio e sulle tecnologie utilizzate, in particolar modo se innovative.

B) TIPOLOGIA DI DATI TRATTATI

Tenendo conto di eventuali altri trattamenti in essere l'attività di raccolta informazioni deve quindi essere completata con le seguenti valutazioni sulle tipologie di dati trattati:

- Il progetto implica il trattamento di dati personali?

  Per dato personale si intende un dato che riguarda l'individuo (persona fisica) - nomi, immagini, indirizzi, ecc.
  Definizione GDPR «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

- Il progetto implica il trattamento di dati sensibili o dati giudiziari?

  Per dato sensibile (artt. 9 “dati particolari” e 10 GDPR) si intendono dati personali particolarmente delicati in quanto riguardanti la sfera personale dell'individuo.
  Definizione CP dati sensibili: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
  Definizione GDPR: dati che rivelino l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all’orientamento sessuale della persona.

- I dati personali vengono raccolti direttamente dall'interessato o anche da altre fonti? - Se **NO**, ad esempio perché i dati non sono raccolti direttamente dall'interessato ma provengono anche da altre fonti (ad es. acquisto di data base, dati pubblici, dati raccolti su web, ecc.), specificare da che fonti i dati sono raccolti.

- Il progetto prevede trattamenti di profilazione o scoring? - Se si specificare quali.

  Il riferimento è a meccanismi di profilazione o algoritmi predittivi che possano ad esempio impattare sulla situazione economica, sulla salute, sugli interessi personali, sul comportamento, sull'ubicazione, sugli spostamenti, sulle abitudini di consumo, sul rendimento professionale, ecc.

- Il progetto prevede decisioni automatizzate che possano produrre effetti giuridici? Se si specificare quali.

  Il riferimento è ad algoritmi di decisione automatica che possano comportare effetti giuridici per i destinatari (ad es. esclusione da un contratto, da determinati benefici, ecc.) senza l'intervento di decisione umana.

C) ANALISI DEL TRATTAMENTO DEI DATI.

- Il progetto prevede attività di monitoraggio sistematico o videosorveglianza? Se si specificare quali.

  Il riferimento è a logiche che consentono di osservare, monitorare e controllare gli interessati (ad esempio monitoraggio di aree accessibile al pubblico, riprese di videosorveglianza, ecc.).

- Il progetto prevede trattamenti su larga scala? Se si specificare quali.

il riferimento è a trattamenti su grandi quantità di dati, tenendo in considerazione il numero di soggetti interessati, il volume dei dati, l'ambito geografico, ecc. La legge non specifica il concetto di larga scala ma un indicatore può essere la gestione di più di 5000 dati.

- Il progetto prevede il trattamento di dati relativi a interessati potenzialmente vulnerabili? Se si specificare quali.

  il riferimento è a trattamenti di dati relativi a interessati potenzialmente vulnerabili o che difficilmente siano in grado di far valere i propri diritti (ad esempio minori, anziani, pazienti, ecc.

- Il progetto prevede l'utilizzo di nuove tecnologie o soluzioni organizzative innovative? Se si specificare quali.

  il riferimento è all'uso di tecnologie innovative rispetto allo stato dell'arte o a forme innovative di raccolta e di utilizzo dei dati.

- Il progetto prevede il trattamento di dati genetici o biometrici? Se si specificare quali.

  Dati genetici: il riferimento è a dati idonei a identificare patologie genetiche, malattie ereditarie, fattori di rischio genetico;
  Dati biometrici: il riferimento ai è a dati idonei a riconoscere iride o retina, impronte digitali, rilevazione facciale, rilevazione di andatura, movimento labbra, ecc.

- Il progetto prevede attività di geo-localizzazione o geo-referenziazione? Se si specificare quali.

  Il riferimento è a dati idonei a identificare la posizione di persone o beni.

- Il progetto prevede elaborazione di dati finanziari relativi all'interessato? Se si specificare quali.

  Il riferimento è a dati idonei a processi che possano implicare elaborazione di dati finanziari dell'interessato (ad es. dati relativi a carta di credito nell'ambito di transazioni di pagamento).
  Si sono già identificati in fase di pre-analisi del progetto rischi specifici che il progetto potrebbe comportare per i diritti e le libertà delle persone. Indicare se in fase di pre-analisi si sono già identificate particolari categorie di rischio rispetto ai dati personali trattati (es. rischio che minori facciano uso non autorizzato del servizio, rischi che terze parti coinvolte nel progetto possano utilizzare i dati in modo improprio, ecc.).

D) RESPONSABILITÀ PER UTILIZZO DEI DATI E FLUSSI INTERNAZIONALI

- Chi è il titolare dei dati acquisiti nel progetto? Specificare per quali Società vengono raccolti i dati e quali sono le Funzioni aziendali che gestiranno i dati raccolti. Indicare se i dati verranno condivisi con l'Outsourcer o soggetti terzi.

- I dati potranno essere condivisi con terze parti? - Specificare se i dati potranno essere condivisi con terze parti (società o professionisti esterni), indicare tali terze parti e specificare qual è il ruolo di ogni terza parte coinvolta nel trattamento dei dati.

  Specificare se le terze parti (ad esempio provider esterni) avranno il diritto di scegliere o modificare gli scopi per i quali i dati vengono utilizzati (ad es. per progetti diversi rispetto a quello per cui collaborano con la Società) o se dovranno attenersi ai vincoli forniti dal titolare.
  Specificare inoltre se si prevede che vi siano soggetti incaricati di elaborare i dati per conto della Società (ad esempio per analisi statistiche o ricerche di mercato).

- I dati potranno essere condivisi con organizzazioni situate al di fuori dell'Unione Europea? Se si indicare quali organizzazioni e in quali Paesi extra UE.

E) FINALITÀ E MODALITÀ DEL TRATTAMENTO

- Descrivere lo scopo per cui sono trattati i dati personali?

Descrivere lo scopo per cui i dati personali vengono acquisiti nell'ambito del progetto ad un livello ragionevole di dettaglio (specificare se i dati sono raccolti per l'erogazione di servizio, ai fini promozionali o marketing, per la gestione di eventi, ecc.).

- Come si prevede che i dati siano manutenuti e aggiornati?

  Descrivere il modo in cui i dati saranno raccolti, mantenuti e aggiornati. Specificare se i dati sono conservati in data base interni o esterni, su cloud, ecc.

- Spiegare con che logiche i dati potranno essere aggiornati e da chi?

- Allo stato delle informazioni disponibili per quanto tempo si prevede di conservare i dati?

  Indicare, se già note, le tempistiche di conservazione dei dati ai fini del progetto. Specificare, se già note, le modalità in cui i dati saranno cancellati al termine dell'utilizzo. Se non si hanno informazioni allo stato indicare: valutazione per ora non disponibile.

- In che modo gli interessati possono accedere ai propri dati?

  Specificare, se già note, le modalità con cui gli interessati potranno accedere ai propri dati (ad es. gestione di richieste di accesso anagrafico, possibilità di modificare direttamente i propri profili, ecc.

F) DIRITTI DEGLI INTERESSATI

- È prevista la predisposizione di un'apposita informativa agli interessati e l'acquisizione del consenso degli stessi al trattamento dei dati?

  - Se **SI** specificare, se già note, le modalità con cui saranno predisposte le informative e le dichiarazioni di consenso;
  - Se **NO** indicare perché il trattamento si ritiene comunque legittimo. Specificare in caso di assenza di acquisizione del consenso perché il trattamento dei dati personali si ritiene comunque legittimo (ad es. dai necessari per conformità ad obblighi di legge, dati necessari per protezione e sicurezza individui, legittimo interesse da parte del titolare che non pregiudica gli interessi degli individui, ecc.).

- Il progetto prevede il trattamento di dati personali per i quali il consenso agli interessati sia stato richiesto da terze parti? - Se **SI** specificare quali tutele sono state assunte per verificare l'effettiva acquisizione del consenso da parte della terza parte.

G) MISURE TECNICHE E ORGANIZZATIVE PER LA SICUREZZA DEI DATI

- Quali misure organizzative saranno predisposte per assicurare la sicurezza dei dati?

  Specificare se già note, le misure fisiche e organizzative predisposte per garantire la sicurezza dei dati (es. dati archiviati sotto chiave, accesso fisico con badge, ruoli e profili utenti per accesso ai dati e per il trattamento e incaricati del trattamento identificati).

- Quali misure tecniche saranno predisposte per assicurare la sicurezza dei dati?

  Specificare se già note, le misure tecniche predisposte per garantire la sicurezza dei dati.
  Indicare le IT policy che verranno applicate e le misure di sicurezza specifiche (ad esempio crittografia dei dati, procedure per identificare violazioni di sicurezza, ecc.).

3. FASE II - VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

- Data di compilazione - inserire data compilazione;
- Nome del progetto - inserire nome progetto;
- Funzione che ha in carico il progetto - inserire una Funzione che ha una visione complessiva e che ha in carico il progetto.

Fase	A cosa serve	Chi	Come	Quando
FASE II Valuta	Con gli elementi raccolti in fase I, serve a decidere se attivare o meno una valutazione di impatto	Funzione richiedente + IT + Legal + DPO/Privacy Champion	A mezzo di confronto con il DPO/Privacy Champion e compilazione esito di fase II	Al termine della fase I e comunque prima dell'inizio del trattamento dei dati

A) ALLA LUCE DELLE INFORMAZIONI FORNITE IN *FASE I* È NECESSARIO PROCEDERE CON UNA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI?

Se **SI** passare a ***FASE III;***

- Se NO indicare approfonditamente le ragioni per cui non si ritiene necessario procedere. Specificare in maniera analitica le ragioni per cui non si ritiene necessario procedere: le valutazioni devono essere condivise da tutto il team di progetto.

B) FIRMA COMPONENTI GRUPPO DI LAVORO

- Responsabile della Protezione dei dati (DPO) - Inserire nome e firma;
- Responsabile Servizi Informatici – Inserire nome e firma;
- Responsabile AFC – Inserire nome e firma;
- Responsabile SEGRETERIA GENERALE - Inserire nome e firma;
- Resp. Funzione che ha incarico il progetto - Inserire nome e firma;
- Inserire altre Funzioni che si ritiene di volta in volta opportuno coinvolgere nella valutazione.

4. FASE III – APPROFONDIMENTO DELLA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

- Data di compilazione - inserire data compilazione;
- Nome del progetto - inserire nome progetto;
- Funzione che ha in carico il progetto - inserire una Funzione che ha una visione complessiva e che ha in carico il progetto.

Fase	A cosa serve	Chi	Come	Quando
FASE III Approfondisci	Serve ad effettuare la valutazione di impatto	Funzione richiedente + IT + Legal	A mezzo checklist della fase III	Prima dell'inizio del trattamento dei dati

A) DESCRIZIONE DEL TRATTAMENTO PREVISTO

- Descrizione sistematica delle finalità del trattamento.

  Inserire una descrizione sistematica delle finalità del trattamento (scopo per cui i dati personali sono trattati).

- Progetto nell'ambito del quale sarà effettuato il trattamento.

  Inserire una descrizione sintetica del progetto nell'ambito del quale sarà effettuato il trattamento.

- Perimetri geografici - Specificare se il progetto:

  - si rivolge o meno a individui situati in Europa;
  - prevede o meno il coinvolgimento di partner o provider extra europei (incluse eventuali altre Società del Gruppo);
  - prevede il trasferimento di dati personali al di fuori dell'Unione Europea e se SI in che Paesi.

- Modalità di trattamento e di elaborazione dei dati - Specificare analiticamente le modalità di trattamento distinguendo:

  - modalità di trattamento manuali da modalità di trattamento con sistemi informatici;
  - asset, sistemi e strumenti con cui le diverse fasi di trattamento sono gestite (hardware e software);
  - eventuali servizi di cloud utilizzati e caratteristiche degli stessi;
  - risorse coinvolte e canali di trasmissione dei dati;
  - ogni ulteriore informazione ritenuta utile per la descrizione tecnica delle modalità di trattamento.

- Tempi di conservazione dei dati e modalità di cancellazione.

  Specificare i tempi di conservazione dei dati e le modalità con cui i dati saranno cancellati al termine dell'utilizzo.

B) VALUTAZIONE DELLE NECESSITÀ E PROPORZIONALITÀ DEL TRATTAMENTO

- Necessità e proporzionalità del trattamento.

  Specificare i motivi per cui il trattamento si rende necessario e i criteri di proporzionalità dello stesso (ad esempio limitazione dei dati acquisiti rispetto alle sole finalità per cui i dati sono trattati).

- È stata effettuata una consultazione preventiva con gli interessati al trattamento? Se no spiegare le ragioni per cui la consultazione non si è resa necessaria (ad es. riservatezza dei progetti aziendali, consultazione sproporzionata o impraticabile, ecc.).

C) SOGGETTI E RESPONSABILITÀ

- Titolare del trattamento.

  Indicare il Titolare del trattamento e le principali Funzioni che all'interno della Società saranno incaricate di trattare i dati personali. Specificare casi di eventuali contitolarità del trattamento.

- Terze parti.

Indicare le terze parti coinvolte come Responsabili del Trattamento, i provider di servizi tecnici o IT e le terze parti cui i dati potranno essere eventualmente comunicati, specificando le responsabilità di tali parti nel trattamento dei dati.

D) TIPOLOGIE DI DATI PERSONALI TRATTATI

- I dati personali vengono raccolti direttamente dall'interessato o anche da altre fonti?

  Specificare se i dati vengono raccolti direttamente dall'interessato o pure da fonti esterne o ancora in forma mista (ad es. dati forniti da interessato poi completati con dati raccolti da fonti esterne).

  Il progetto prevede il trattamento delle seguenti categorie di dati personali o le seguenti attività. NB: le informazioni devono essere confrontate con quelle fornite in ***FASE I*** se vi sono differenzi tra le due fasi (ad es. categorie di dati che si pensava di utilizzare ma che non saranno utilizzate, specificare tali differenze.

  - Dati "Sensibili" ("Particolari" ex art. 9 GDPR) o Giudiziari - Commenti e dettagli;
  - Trattamenti su Larga Scala - Commenti e dettagli;
  - Attività di Profilazione o Scoring - Commenti e dettagli;
  - Decisioni Automatizzate con Effetti Giuridici - Commenti e dettagli;
  - Monitoraggio Sistematico o Videosorveglianza - Commenti e dettagli;
  - Dati Relativi a Interessati Vulnerabili - Commenti e dettagli;
  - Uso Di Nuove Tecnologie o Soluzioni Innovative - Commenti e dettagli;
  - Dati Genetici o Biometrici - Commenti e dettagli;
  - Attività Di Geo-Localizzazione o Geo- Referenziazione - Commenti e dettagli;
  - Dati Finanziari o Relativi a Strumenti Di Pagamento - Commenti e dettagli.

E) RISCHI PER DIRITTI E LIBERTÀ E MISURE PREVISTE PER AFFRONTARE I RISCHI

Le valutazioni di rischio devono associare elementi di probabilità e elementi di gravità (impatto) sul trattamento dei dati. Questi ultimi devono essere considerati anche alla luce della tipologia di dati gestiti (più o meno sensibili) e agli impatti che potrebbero derivare sui diritti e sulle libertà degli interessati.

- Rischi che i dati possano essere trattati in modo illegittimo all'interno dell'organizzazione o che gli interessati possano essere non adeguatamente informati sul trattamento dei loro dati.

Probabilità	
Impatto	
Rischi inerenti	
Rischi residuali	

Misure tecniche e organizzative adottate → Descrivere le misure tecniche e organizzative già implementate per ridurre il rischio.

- Rischi che i dati possano essere utilizzati non rispettando i limiti delle finalità per cui sono raccolti o che vengano raccolti dati eccedenti le finalità previste dal progetto.

Probabilità	
Impatto	
Rischi inerenti	
Rischi residuali	

Misure tecniche e organizzative adottate → Descrivere le misure tecniche e organizzative già implementate per ridurre il rischio.

- Rischi che i dati possano essere non completi o non accurati, che possano essere cancellati o modificati senza ragione o che sia difficile procedere al loro aggiornamento.

Probabilità	
Impatto	
Rischi inerenti	
Rischi residuali	

Misure tecniche e organizzative adottate → Descrivere le misure tecniche e organizzative già implementate per ridurre il rischio.

- Rischi che i dati siano conservati per un periodo non necessario rispetto al trattamento.

Probabilità	
Impatto	
Rischi inerenti	
Rischi residuali	

Misure tecniche e organizzative adottate → Descrivere le misure tecniche e organizzative già implementate per ridurre il rischio.

- Rischi che l'interessato possa avere difficoltà ad esercitare i suoi diritti (es. diritto alla cancellazione o modifica del dato) o che i suoi diritti vengano violati.

Probabilità	
Impatto	
Rischi inerenti	
Rischi residuali	

Misure tecniche e organizzative adottate → Descrivere le misure tecniche e organizzative già implementate per ridurre il rischio.

- Rischi di sicurezza fisica dei dati (sottrazione, perdita, alterazione, manomissione, accesso abusivo) all'interno dell'organizzazione.

Probabilità	
Impatto	
Rischi inerenti	
Rischi residuali	

Misure tecniche e organizzative adottate → Descrivere le misure tecniche e organizzative già implementate per ridurre il rischio.

- Rischi di sicurezza informatica dei dati (sottrazione, perdita, alterazione, manomissione, accesso abusivo ai sistemi) all'interno dell'organizzazione.

Probabilità	
Impatto	
Rischi inerenti	
Rischi residuali	

Misure tecniche e organizzative adottate → Descrivere le misure tecniche e organizzative già implementate per ridurre il rischio.

- Rischi di sicurezza fisica e informatica relativi alle terze parti coinvolte nel progetto.

Probabilità	
Impatto	
Rischi inerenti	
Rischi residuali	

Misure tecniche e organizzative adottate → Descrivere le misure tecniche e organizzative già implementate per ridurre il rischio.

5. FASE IV – FINALIZZAZIONE DELLA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

RISULTATI VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

- Data di compilazione - inserire data compilazione;
- Nome del progetto - inserire nome progetto;
- Funzione che ha in carico il progetto - inserire una Funzione che ha una visione complessiva e che ha in carico il progetto.

Fase	A cosa serve	Chi	Come	Quando
FASE IV Finalizza e chiudi la valutazione	Serve a valutare gli esiti della valutazione di impatto e decidere le azioni conseguenti (ad esempio comunicazioni alle autorità)	Funzione richiedente + IT + Legal + DPO/Privacy Champion	A mezzo di confronto con il DPO/Privacy Champion e compilazione esito di fase IV	Prima dell'inizio del trattamento dei dati

A) SINTESI DEI RISCHI RESIDUALI PER DIRITTI E LIBERTÀ ALLA LUCE DELLE MISURE TECNICHE E ORGANIZZATIVE GIÀ IMPLEMENTATE

- Rischi che i dati possano essere trattati in modo illegittimo all'interno dell'organizzazione o che gli interessati possano essere non adeguatamente informati sul trattamento dei loro dati.

Rischi inerenti	

Rischi residuali alla luce delle misure tecnico-organizzative già implementate	

- Ulteriori misure suggerite caso di rischio residuale **MEDIO** → Indicare le misure suggerite in caso di rischio residuale, i tempi stimati di realizzazione delle stesse e le responsabilità conseguenti assegnate;

- Ulteriori misure raccomandate in caso di rischio residuale **ALTO** → Indicare le misure **RACCOMANDATE** in caso di rischio residuale ALTO, i tempi stimati di realizzazione delle stesse e le responsabilità conseguenti assegnate.

- Rischi che i dati possano essere utilizzati non rispettando i limiti delle finalità per cui sono raccolti o che vengano raccolti dati eccedenti le finalità previste dal progetto.

Rischi inerenti	
Rischi residuali alla luce delle misure tecnico-organizzative già implementate	

- Ulteriori misure suggerite caso di rischio residuale **MEDIO** → Indicare le misure suggerite in caso di rischio residuale, i tempi stimati di realizzazione delle stesse e le responsabilità conseguenti assegnate;

- Ulteriori misure raccomandate in caso di rischio residuale **ALTO** → Indicare le misure **RACCOMANDATE** in caso di rischio residuale ALTO, i tempi stimati di realizzazione delle stesse e le responsabilità conseguenti assegnate.

- Rischi che i dati possano essere non completi o non accurati, che possano essere cancellati o modificati senza ragione o che sia difficile procedere al loro aggiornamento.

Rischi inerenti	
Rischi residuali alla luce delle misure tecnico-organizzative già implementate	

- Ulteriori misure suggerite caso di rischio residuale **MEDIO** → Indicare le misure suggerite in caso di rischio residuale, i tempi stimati di realizzazione delle stesse e le responsabilità conseguenti assegnate;

- Ulteriori misure raccomandate in caso di rischio residuale **ALTO** → Indicare le misure **RACCOMANDATE** in caso di rischio residuale ALTO, i tempi stimati di realizzazione delle stesse e le responsabilità conseguenti assegnate.

- Rischi che i dati siano conservati per un periodo non necessario rispetto al trattamento.

- Ulteriori misure suggerite caso di rischio residuale **MEDIO** → Indicare le misure suggerite in caso di rischio residuale, i tempi stimati di realizzazione delle stesse e le responsabilità conseguenti assegnate;

- Ulteriori misure raccomandate in caso di rischio residuale **ALTO** → Indicare le misure **RACCOMANDATE** in caso di rischio residuale ALTO, i tempi stimati di realizzazione delle stesse e le responsabilità conseguenti assegnate.

- Rischi che l'interessato possa avere difficoltà ad esercitare i suoi diritti (es. diritto alla cancellazione o modifica del dato) o che i suoi diritti vengano violati.

Rischi inerenti	
Rischi residuali alla luce delle misure tecnico-organizzative già implementate	

- Ulteriori misure suggerite caso di rischio residuale **MEDIO** → Indicare le misure suggerite in caso di rischio residuale, i tempi stimati di realizzazione delle stesse e le responsabilità conseguenti assegnate;

- Ulteriori misure raccomandate in caso di rischio residuale **ALTO** → Indicare le misure **RACCOMANDATE** in caso di rischio residuale ALTO, i tempi stimati di realizzazione delle stesse e le responsabilità conseguenti assegnate.

- Rischi di sicurezza fisica dei dati (sottrazione, perdita, alterazione, manomissione, accesso abusivo) all'interno dell'organizzazione.

- Ulteriori misure suggerite caso di rischio residuale **MEDIO** → Indicare le misure suggerite in caso di rischio residuale, i tempi stimati di realizzazione delle stesse e le responsabilità conseguenti assegnate;

- Ulteriori misure raccomandate in caso di rischio residuale **ALTO** → Indicare le misure **RACCOMANDATE** in caso di rischio residuale ALTO, i tempi stimati di realizzazione delle stesse e le responsabilità conseguenti assegnate.

- Rischi di sicurezza informatica dei dati (sottrazione, perdita, alterazione, manomissione, accesso abusivo ai sistemi) all'interno dell'organizzazione.

Rischi inerenti	
Rischi residuali alla luce delle misure tecnico-organizzative già implementate	

- Ulteriori misure suggerite caso di rischio residuale **MEDIO** → Indicare le misure suggerite in caso di rischio residuale, i tempi stimati di realizzazione delle stesse e le responsabilità conseguenti assegnate;

- Ulteriori misure raccomandate in caso di rischio residuale **ALTO** → Indicare le misure **RACCOMANDATE** in caso di rischio residuale ALTO, i tempi stimati di realizzazione delle stesse e le responsabilità conseguenti assegnate.

- Rischi di sicurezza fisica e informatica relativi alle terze parti coinvolte nel progetto.

Rischi inerenti	

Rischi residuali alla luce delle misure tecnico-organizzative già implementate	

- Ulteriori misure suggerite caso di rischio residuale **MEDIO** → Indicare le misure suggerite in caso di rischio residuale, i tempi stimati di realizzazione delle stesse e le responsabilità conseguenti assegnate;

- Ulteriori misure raccomandate in caso di rischio residuale **ALTO** → Indicare le misure **RACCOMANDATE** in caso di rischio residuale ALTO, i tempi stimati di realizzazione delle stesse e le responsabilità conseguenti assegnate.

B) VALUTAZIONE FINALE

- Responsabile della Protezione dei dati (DPO) - Inserire nome e firma;
- Responsabile Servizi Informatici – Inserire nome e firma;
- Responsabile AFC – Inserire nome e firma;
- Responsabile SEGRETERIA GENERALE - Inserire nome e firma;
- Resp. Funzione che ha incarico il progetto - Inserire nome e firma;
- Inserire altre Funzioni che si ritiene di volta in volta opportuno coinvolgere nella valutazione.

Valutazione Finale condivisa con il Responsabile della Protezione dei dati (DPO). Alla luce delle informazioni raccolte e dei risultati della
presente valutazione di impatto:

☐ *E' possibile procedere con l'implementazione del progetto e l'avvio del trattamento senza ulteriori misure tecniche e organizzative.*

☐ *E' possibile procedere con l'implementazione del progetto e l'avvio del trattamento senza ulteriori misure tecniche e organizzative ma si suggerisce di implementare le misure tecniche e organizzative sopra indicate.*

☐ *E' possibile procedere con l'implementazione del progetto e l'avvio del trattamento solo dopo aver implementato le misure tecniche e organizzative ulteriori sopra indicate e previa verifica delle seguenti azioni.*

Specificare come si intende monitorare l'implementazione delle misure di follow-up raccomandate e rispetto a quali scadenze.

☐ *E' necessario consultare l'attività di controllo prima di iniziare il trattamento.*

- Responsabile della Protezione dei dati (DPO) - Inserire nome e firma;
- Legale Rappresentante Titolare - Inserire nome e firma.

6. ALLEGATI

Numero allegato (acronimo)	Descrizione allegato (nome esteso)	File
Allegato 1	M4 DPIA_checklist	