GDPRLab PRO

Guida Operativa

Sezione: DPIA – Data Protection Impact Assessment

Campo	Valore
Piattaforma	GDPRLab
Sezione	DPIA
Destinatari	Consulenti tecnici / DPO / Rivenditori
Versione guida	1.1 (completa)

1

1. Cos’è la sezione DPIA

La sezione DPIA (Data Protection Impact Assessment – Valutazione d’Impatto sulla Protezione dei Dati) consente di condurre e documentare le valutazioni di impatto previste dall’art. 35 GDPR per i trattamenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

La DPIA è un processo per identificare e minimizzare i rischi per i diritti delle persone. È obbligatoria quando il trattamento può presentare un rischio elevato per i diritti e le libertà (art. 35 GDPR).

Si accede cliccando su **DPIA** nel menu laterale sinistro.

> ***Nota operativa:*** *Le DPIA completate non vengono visualizzate in forma editabile in questa sezione: vengono generate come documenti PDF certificati e archiviate automaticamente nel Repository Documenti con impronta SHA-256, numero seriale e data certificata. Per consultare una DPIA esistente, accedere al Repository e filtrare per categoria DPIA.*

2

2. Pagina principale

La pagina mostra:

→ **Card KPI Totale DPIA** – numero di valutazioni create

→ **Box informativo** con la definizione di DPIA e riferimento normativo (art. 35 GDPR)

→ **Griglia di card**: una per ogni trattamento per cui è stata avviata o completata una DPIA

→ Pulsante **+ Nuova DPIA** in alto a destra

Ogni card mostra il nome del trattamento (es. “Trattamento: Dipendenti”, “Trattamento: Registrazioni videosorveglianza”). Cliccando sulla card si accede alla DPIA di quel trattamento per modificarla o completarla.

3

3. Struttura della DPIA generata da GDPRLab

GDPRLab genera automaticamente un documento PDF strutturato seguendo la metodologia indicata dalle Linee guida WP248 dell'EDPB e il Provvedimento del Garante n. 467 dell'11 ottobre 2018. Il documento comprende le seguenti sezioni principali:

Sezione	Contenuto
Nozione di valutazione d'impatto	Definizione della DPIA e inquadramento come strumento di accountability
Quadro normativo	Riferimenti normativi: art. 35 e 36 GDPR, considerando C84-C95, WP248, Provvedimento Garante n. 467/2018
Motivi della valutazione d'impatto	Motivo per cui il trattamento specifico richiede una DPIA (criterio applicabile da WP248)
Metodo di conduzione della DPIA	Metodologia adottata, consultazione del DPO, struttura del documento
Valutazione preliminare	Fase 1: Descrizione del trattamento / Fase 2: Valutazione della conformità / Fase 3: Decisione se condurre la DPIA
Esecuzione DPIA	Fase 1: Informazioni integrative / Fase 2: Valutazione del rischio (metodologia RN) / Fase 3: Valutazione idoneità misure di sicurezza
Risultati DPIA	Livello di rischio normalizzato finale; obbligo o meno di comunicazione al Garante
Revisione e aggiornamento	Condizioni che richiedono il riesame della DPIA
Appendice	Tabella riepilogativa dei rischi con rischi residui; misure in via di implementazione; firma del DPO

4

4. Valutazione Preliminare – le tre fasi

Fase 1 – Descrizione del trattamento

La prima fase raccoglie le informazioni di base sul trattamento oggetto di valutazione, attingendo automaticamente dai dati già inseriti nel wizard Trattamenti:

Elemento	Contenuto / Fonte
Soggetti interessati	Categorie di persone i cui dati vengono trattati (es. Prospect, Dipendenti, Clienti)
Finalità del trattamento	Descrizione precompilata dal wizard Trattamenti step 4 (Registro), adattabile
Descrizione del trattamento e flussi informativi	Tipo di dato, formato (digitale/cartaceo), generazione automatica dal dato personale
Dati oggetto del trattamento	Categorie di dati (es. personale_comune, dati sensibili)
Modalità di trattamento	Digitale / Cartaceo / Entrambe
Operazioni eseguite	Elenco degli incaricati al trattamento con i relativi permessi (inserimento, registrazione, modifica, cancellazione, lettura, consultazione, creazione, comunicazione)
Conservazione dei dati trattati	Periodo di conservazione previsto

> ***Nota operativa:*** *I dati della Fase 1 vengono precompilati automaticamente dalla piattaforma attingendo dalle informazioni inserite nel wizard Trattamenti. Verificarne la correttezza e completarli se necessario prima di procedere.*

Fase 2 – Valutazione della conformità

La seconda fase valuta la conformità del trattamento al GDPR. Comprende:

Elemento	Contenuto
Soggetti che hanno accesso ai dati	Elenco incaricati con permessi specifici per banca dati
Modalità di trasferimento a terzi	Indica se e come i dati vengono trasferiti a soggetti terzi
Modalità di aggiornamento e eliminazione	Procedure di aggiornamento, cancellazione e distruzione dei dati

Base giuridica del trattamento	Base giuridica applicabile (es. Consenso, Obbligo legale, Interesse legittimo)
Asset a supporto del trattamento	Hardware, software, archivi, reti e piattaforme utilizzati
Periodo massimo di conservazione	Durata della conservazione dei dati
Misure di sicurezza	Misure organizzative, fisiche e logiche adottate
Trasferimento extra UE	Presenza o meno di trasferimenti verso paesi non UE
Diritti degli interessati	Elenco dei diritti esercitabili (accesso, rettifica, cancellazione, portabilità, opposizione, ecc.)
Principi GDPR rispettati	Checklist dei principi applicati: legalità, minimizzazione, esattezza, limitazione, ecc.

Fase 3 – Decisione: condurre la DPIA?

Sulla base delle risultanze della valutazione preliminare, la piattaforma determina se il trattamento richiede l'esecuzione della DPIA completa. La decisione viene motivata nel documento con riferimento ai criteri applicabili (WP248) e alla storia del trattamento.

In questa fase viene anche presentata la tabella dei 4 rischi principali che verranno analizzati nella fase successiva:

→ Danneggiamento / perdita / distruzione non autorizzata dati personali

→ Accesso non autorizzato dati personali

→ Trattamento non autorizzato (comprensivo di modifica, divulgazione, ecc.)

→ Trattamento non conforme alla finalità della raccolta o illecito

5

5. Esecuzione DPIA – Metodologia di valutazione del rischio

GDPRLab applica una metodologia quantitativa basata su tre fattori per calcolare il Rischio Normalizzato (RN):

$$RN = f\ (P,\ C,\ V)$$

Fattore	Simbolo	Scala	Valori
Probabilità di accadimento	P	1–4	1 = Improbabile / 2 = Poco probabile / 3 = Probabile / 4 = Quasi certo
Conseguenze dell'evento	C	1–4	1 = Trascurabili / 2 = Marginali / 3 = Limitate / 4 = Gravi
Vulnerabilità (adeguatezza misure)	V	3 valori	0,25 = Adeguate / 0,5 = Parzialmente adeguate / 1 = Inadeguate

5.1 Rischio Intrinseco (Ri = P × C)

Il Rischio Intrinseco è il prodotto della Probabilità per le Conseguenze, calcolato prima di considerare le misure di sicurezza adottate:

Ri = P × C	Livello di rischio intrinseco
1 ≤ Ri ≤ 2	Molto basso
3 ≤ Ri ≤ 4	Basso
6 ≤ Ri ≤ 9	Rilevante
12 ≤ Ri ≤ 16	Alto

5.2 Rischio Normalizzato (RN = Ri × V)

Il Rischio Normalizzato tiene conto dell'adeguatezza delle misure di sicurezza adottate: RN = Ri × V (valore peggiore delle misure per quel rischio specifico).

RN = Ri × V	Livello di rischio normalizzato
0,25 ≤ RN ≤ 1	Molto basso
1 < RN < 3	Basso
3 ≤ RN ≤ 9	Rilevante

12 ≤ RN ≤ 16	Alto

> ***Nota operativa:*** *La metodologia RN = f(P, C, V) permette di ridurre significativamente il livello di rischio attraverso misure di sicurezza adeguate (V = 0,25). Un trattamento con rischio intrinseco Alto (Ri = 12–16) e misure adeguate (V = 0,25) produce un RN massimo di 4, classificato come Rilevante anziché Alto.*

5.3 Aree di pericolo analizzate

Area di pericolo	Rischi generati
Agenti fisici (incendio, allagamento, attacchi esterni)	Danneggiamento, perdita, distruzione non autorizzata
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	Danneggiamento, perdita, distruzione non autorizzata
Interruzione servizi (sbalzi tensione, guasti, interruzione rete)	Danneggiamento, perdita, distruzione non autorizzata
Problemi tecnici (anomalie software, hardware, servizio IT)	Danneggiamento, perdita, distruzione, accesso non autorizzato
Compromissione informazioni (intercettazioni, infiltrazioni email)	Perdita, distruzione, accesso non autorizzato
Azioni non autorizzate (errori, virus, uso non autorizzato)	Danneggiamento, perdita, distruzione, accesso non autorizzato, trattamento non autorizzato, trattamento non conforme

5.4 Valutazione delle misure di sicurezza

Per ogni rischio identificato, la piattaforma valuta l'idoneità delle misure di sicurezza adottate, distinte tra trattamenti con strumenti elettronici e trattamenti senza strumenti elettronici:

Trattamenti con strumenti elettronici:

→ **Backup e Disaster Recovery:** procedure e software di backup adeguati

→ **Accesso fisico, organizzativo e logico:** vigilanza sedi, custodia in armadi, controllo accessi, identificazione utente, antivirus, monitoraggio sessioni

→ **Gestione credenziali:** identificazione incaricato, sostituzione periodica, disattivazione codici in caso di perdita qualità o inattività >6 mesi

→ **Conformità finalità:** aggiornamento periodico banche dati, cancellazione dati non occorrenti, cifratura dati sensibili (VPN)

Trattamenti senza strumenti elettronici:

→ Documenti personali mai incustoditi su scrivanie; riporre documenti e attivare salvaschermo in presenza di estranei

→ Incaricati autorizzati solo ai dati strettamente necessari; divieto di raccogliere dati non pertinenti

→ Aggiornamento periodico banche dati; documenti con dati non occorrenti distrutti

6

6. Risultati della DPIA

Il documento DPIA si conclude con una sezione Risultati che riporta:

→ Il livello di rischio normalizzato complessivo del trattamento (es. Rilevante)

→ La valutazione sull'obbligo o meno di comunicazione preventiva al Garante (art. 36 GDPR)

→ L'indicazione che i risultati sono illustrati in appendice

Esempio di risultato: "A valle dell'indagine DPIA condotta l'attività ricade in fascia Rilevante, che tuttavia non è tale da dover prevedere l'obbligo di comunicazione al Garante."

> **Attenzione: Se il livello di rischio normalizzato finale è Alto (RN 12–16), il Titolare è obbligato a consultare preventivamente il Garante prima di avviare il trattamento (art. 36 GDPR). Il trattamento non deve essere avviato fino al ricevimento del parere.**

7

7. Appendice del documento DPIA

Il documento DPIA generato da GDPRLab contiene un'appendice strutturata in tre parti:

Parte appendice	Contenuto
1. Tabella dei rischi	Riepilogo di tutti i rischi identificati con: Probabilità, Conseguenze e Livello di rischio iniziali; Opzioni di mitigazione adottate (trattamento con/senza strumenti elettronici); Rischi residui dopo l'applicazione delle misure (Probabilità, Conseguenze, Livello normalizzato)
2. Misure di sicurezza in via di implementazione	Tabella con i rischi residui e le misure aggiuntive pianificate per ridurli ulteriormente (da compilare quando sono previste misure future)
3. Misure ulteriori a tutela della privacy	Misure aggiuntive adottate nell'esercizio dell'attività prevalente

8

8. Documento finale e certificazione

Il documento PDF generato da GDPRLab è un documento legale certificato che include:

→ Dati del Titolare del Trattamento (ragione sociale, indirizzo, P.IVA, codice fiscale)

→ Responsabile elaborazione DPIA e posizione

→ Firma del Responsabile della Protezione dei Dati (DPO) con data

→ Data di redazione della DPIA

→ Data e ora di generazione del documento

→ Numero seriale univoco (es. XF1417)

→ Impronta Hash SHA-256 del documento

→ Data certificata dell'impronta (timestamp di certificazione)

> ***Nota operativa:*** *Il numero seriale e l'hash SHA-256 permettono di identificare univocamente ogni DPIA generata e di verificarne l'integrità nel tempo. Conservare sempre il PDF originale scaricato dal repository: è il documento probatorio che attesta l'avvenuta conduzione della valutazione di impatto.*

9

9. Revisione e aggiornamento della DPIA

La DPIA non è un adempimento una tantum: deve essere riesaminata periodicamente e in presenza di specifiche condizioni. GDPRLab indica nel documento le condizioni che richiedono revisione:

Cambiamenti sulle attività di trattamento

→ Contesto o finalità del trattamento

→ Tipologia di dati personali trattati

→ Destinatari o modalità di raccolta

→ Combinazioni di dati da fonti diverse

→ Trasferimento di dati all'estero

Modifiche ai rischi

→ Presenza di nuove minacce

→ Modifica ai sistemi informativi a supporto del trattamento

→ Soppressione di contromisure esistenti

→ Nuovi scenari di rischio o nuovi potenziali impatti

→ Attuazione di nuove misure di sicurezza tecniche, organizzative o procedurali

Mutamenti nel contesto organizzativo o sociale

→ Qualsiasi cambiamento significativo nel contesto in cui opera l'organizzazione che possa influenzare i rischi per gli interessati.

10

10. Quando è obbligatoria la DPIA

L'art. 35 GDPR prevede l'obbligo di DPIA quando il trattamento può presentare un rischio elevato. Le Linee guida WP248 EDPB identificano i seguenti criteri: in presenza di almeno 2, la DPIA è generalmente necessaria:

Criterio	Esempi pratici
Valutazione o scoring	Profilazione, solvibilità, analisi comportamentale
Decisioni automatizzate con effetti significativi	Scoring automatico che determina accesso a servizi
Monitoraggio sistematico	Videosorveglianza, tracciamento online, GPS su dipendenti
Dati sensibili o altamente personali	Sanitari, genetici, biometrici, condanne penali
Trattamento su larga scala	Grandi quantità di dati o numerose persone coinvolte
Combinazione o confronto di dataset	Incrocio di dati provenienti da fonti diverse
Dati relativi a soggetti vulnerabili	Minori, pazienti, dipendenti, anziani
Uso innovativo o nuove tecnologie	IoT, AI, biometria, riconoscimento facciale
Trasferimento extra UE	Dati trasferiti verso paesi senza adeguate garanzie

> ***Nota operativa:*** *Il Garante italiano ha pubblicato l'elenco delle tipologie di trattamenti per cui la DPIA è obbligatoria (Provvedimento n. 467 dell'11 ottobre 2018 – G.U. 269 del 19/11/2018). Verificarlo sempre prima di applicare i criteri WP248.*

11

11. Workflow consigliato

→ Completare il wizard Trattamenti: i dati inseriti (tipo dati, misure di sicurezza, accessi, collocazione) alimentano automaticamente la DPIA

→ Identificare i trattamenti che soddisfano almeno 2 criteri WP248 o rientrano nel Provvedimento Garante n. 467/2018

→ Cliccare **+ Nuova DPIA** nella pagina DPIA e selezionare il trattamento

→ Verificare e completare la Fase 1 (descrizione) e la Fase 2 (conformità): i dati sono precompilati ma vanno revisionati

→ Procedere con la Fase 3 (decisione) e l'Esecuzione DPIA con la valutazione del rischio

→ Compilare la sezione sulle misure di sicurezza in via di implementazione (Appendice 2)

→ Ottenere il parere del DPO (se designato) e raccoglierne la firma

→ Completare la DPIA: il sistema genera il PDF con hash SHA-256 e lo archivia nel Repository

→ Per consultare la DPIA: accedere al Repository Documenti e filtrare per categoria DPIA

→ Aggiornare la DPIA ogni volta che si verificano le condizioni di revisione indicate nella sezione 9

12

12. Relazioni con altre sezioni

Sezione	Relazione con la DPIA
Trattamenti	Il wizard Trattamenti precompila automaticamente i dati della Fase 1 e 2 della DPIA (tipo dati, misure, accessi, collocazione)
Registro Trattamenti	Il Registro deve indicare se un trattamento è stato sottoposto a DPIA; la DPIA completa il Registro come documento probatorio
Nomine	Il DPO (se designato) va consultato nella DPIA; il suo parere e la firma sono parte del documento finale
Sicurezza informatica	Le misure di sicurezza configurate (backup, accessi, logging) sono le misure di mitigazione valutate nella DPIA
Repository	Le DPIA completate vengono archiviate con hash SHA-256 e filtro DPIA; è qui che si consultano le DPIA già prodotte
Registro Data Breach	Un breach grave su trattamento con DPIA richiede la revisione della valutazione di impatto
Responsabili Esterni	I responsabili del trattamento coinvolti nel trattamento oggetto di DPIA sono indicati nella Fase 2