Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia DFGP

**Office fédéral de la** justice **OFJ**
Domaine de direction Droit public
Unité Projets législatifs I

**Guida VIPD**

## Indice

## 1 Destinatari della guida

La guida è destinata anzitutto alle unità amministrative dell'Amministrazione federale centrale[1] tenute a effettuare una valutazione d'impatto sulla protezione dei dati (VIPD) ai sensi dell'articolo 22 della legge federale del 25 settembre 2020 sulla protezione dei dati (LPD)[2] e delle direttive del Consiglio federale per l'esame preliminare dei rischi e la valutazione dei dati in caso di trattamento di dati personali da parte dell'Amministrazione federale (direttive VIPD)[3].

Le unità amministrative dell'Amministrazione federale decentralizzata[4], così come le persone incaricate di un compito federale, cui non si applicano le direttive VIPD, sono comunque tenute a rispettare la legge sulla protezione dei dati nella misura in cui sono considerate organi federali[5]. Se sono adempite le condizioni di cui all'articolo 22 LPD, queste diverse unità devono pertanto valutare l'impatto sulla protezione dei dati e a tal fine sono libere di servirsi delle direttive VIPD e degli strumenti ausiliari disponibili, come la presente guida.

La VIPD permette anche di dimostrare che il trattamento dei dati personali previsto tiene conto della protezione dei dati (*privacy by design*)[6]. Inoltre la VIPD consente ai titolari del trattamento di verificare che i dati siano trattati in maniera conforme alle esigenze in materia di protezione dei dati.

**Delimitazione rispetto al promemoria sulla valutazione d'impatto sulla protezione dei dati (VIPD) secondo gli articoli 22 e 23 LPD dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT)**: la guida VIPD dell'UFG concerne unicamente la valutazione d'impatto sulla protezione dei dati da parte dell'Amministrazione federale centrale, mentre il promemoria dell'IFPDT si rivolge anzitutto ai titolari privati del trattamento e può essere consultato dagli organi federali a fini interpretativi.

## 2 Come effettuare una VIPD

### 2.1 Chi deve effettuare una VIPD?

La legge si limita ad affermare che il titolare procede a una VIPD. Conformemente all'articolo 5 lettera j LPD, l'unità amministrativa responsabile è quella che, singolarmente o insieme ad altri, determina lo scopo e i mezzi del trattamento; deve inoltre garantire la realizzazione della VIPD, cui non necessariamente deve provvedere di persona. Poiché una VIPD richiede conoscenze specifiche in vari settori (diritto, informatica, ecc.), idealmente andrebbe realizzata da un'equipe interdisciplinare e competente in materia di protezione dei dati, d'identificazione dei rischi, di processi e sistemi informatici.

---

1 Ai sensi dell'art. 7 dell'ordinanza sull'organizzazione del Governo e dell'Amministrazione (OLOGA, RS **172.010.1**).
Nell'ambito del diritto della protezione dei dati, tali unità sono considerate organi federali (cfr. l'art. 5 lett. i LPD che definisce gli organi federali come «autorità o servizio della Confederazione, oppure persona cui sono affidati compiti federali», RS **235.1**).

2 RS **235.1**.

3 FF **2023** 1882.

4 Ai sensi dell'art. 7*a* OLOGA.

5 Cfr. l'art. 5 lett. i LPD.

6 Art. 7 cpv. 1 e 2 LPD.

Il consulente per la protezione dei dati consiglia inoltre il titolare del trattamento e verifica l'esecuzione della VIPD[7]. È importante coinvolgerlo durante l'intero processo, affinché si tenga adeguatamente conto del diritto della protezione dei dati. Il consulente deve poter esercitare la propria funzione in modo indipendente dall'unità amministrativa responsabile, senza riceverne istruzioni[8].

Il titolare del trattamento deve provvedere alla VIPD anche quando prevede di affidare a un responsabile il trattamento dei dati personali.

### 2.2 Quando effettuare una VIPD?

Una VIPD va eseguita in caso di rischio elevato per i diritti fondamentali della persona interessata. Per stabilire se esiste un rischio elevato, occorre ricorrere allo strumento per l'esame preliminare dei rischi, redatto dall'UFG e illustrante i principali fattori di rischio. Contrariamente a quanto contempla per i titolari privati del trattamento, l'articolo 22 LPD non prevede eccezioni per le unità amministrative, che quindi non possono rinunciare alla VIPD. Se dall'esame preliminare dei rischi emerge un elevato rischio per i diritti fondamentali della persona interessata, occorre una VIPD. Se sono previste più operazioni di trattamento simili, l'articolo 22 capoverso 1 LPD include la possibilità di una VIPD comune.

L'articolo 22 capoverso 1 LPD esige di effettuare la VIPD «previamente». Significa che occorre esaminare i rischi e valutare l'impatto sulla protezione dei dati prima di trattare i dati personali. Idealmente, la VIPD va effettuata quanto prima, anche se non sono ancora noti tutti i parametri del trattamento dei dati, e adeguata durante la fase di pianificazione.

La VIPD andrebbe effettuata non appena l'unità amministrativa responsabile prevede un nuovo trattamento di dati oppure essere un adattamento di un trattamento esistente. Per i trattamenti avviati prima dell'entrata in vigore della nuova LPD, l'articolo 69 prevede una VIPD solo se lo scopo del trattamento cambia o se sono raccolti nuove categorie dei dati.

**Coordinamento con la procedura legislativa (n. 4 direttive VIPD):** se il trattamento dei dati necessita di una nuova base legale o dell'adeguamento di una esistente, la VIPD va effettuata prima dell'elaborazione o modifica, poiché i risultati vanno allegati all'incarto per la consultazione degli uffici. Se la necessità di procedere a una VIPD o di adeguarla emerge solo dopo l'apertura della consultazione degli uffici, i risultati della VIPD sono allegati all'incarto per la consultazione degli uffici successiva o la procedura di corapporto.

**Coordinamento con il metodo di gestione dei progetti HERMES[9] (n. 5 direttive VIPD):** se i dati sono trattati nel quadro di un progetto HERMES, si procede con la VIPD durante la fase concettuale realizzata con metodi classici o agili. HERMES consente inoltre di applicare altri metodi; tuttavia, anche in questo caso, il quadro è definito da HERMES. Nel metodo classico, la fase concettuale corrisponde alla progettazione. Nel metodo agile la VIPD va effettuata durante l'implementazione, preferibilmente in contemporanea con il piano SIPD.

[7] Art. 26 cpv. 2 lett. a n. 2 dell'ordinanza sulla protezione dei dati (OPDa), RS **235.11.**

[8] Art. 26 cpv. 1 lett. b OPDa.

[9] www.hermes.admin.ch.

### 2.3 In quale forma e per quanto tempo occorre conservare la VIPD?

La LPD e l'ordinanza sulla protezione dei dati (OPDa)[10] non forniscono direttive sulla forma della VIPD. Come per gli altri strumenti della LPD e dell'OPDa, compete infatti all'unità amministrativa responsabile stabilire la forma in cui conservare la VIPD. Tuttavia è importante che l'unità possa dimostrare di avere eseguito la VIPD, presentarla all'IFPDT se necessario e allegarne i risultati all'incarto per la consultazione degli uffici. In altri termini, la VIPD e i relativi risultati devono essere disponibili in un formato standard.

In merito alla conservazione della VIPD, l'articolo 14 OPDa stabilisce che l'unità amministrativa responsabile deve conservarla per almeno due anni dopo la fine del trattamento.

### 2.4 Occorre pubblicare la VIPD?

La LPD e l'OPDa non prevedono l'obbligo di pubblicare la VIPD, considerati i dati sensibili che può contenere. La pubblicazione andrebbe tuttavia presa in considerazione al fine di tutelare maggiormente i diritti fondamentali degli interessati, il che è proprio lo scopo di una VIPD. La pubblicazione rende più trasparente il trattamento dei dati personali e rafforza inoltre la fiducia tra gli interessati e i titolari del trattamento. La pubblicazione rientra nel margine discrezionale dell'unità amministrativa responsabile.

Per il resto, le disposizioni della legge 17 dicembre 2004 sulla trasparenza[11] si applicano anche alla VIPD.

**Coordinamento con la procedura legislativa (n. 4 direttive VIPD):** quando la VIPD è effettuata nel quadro di una procedura legislativa, i risultati[12] devono essere allegati all'incarto per la consultazione degli uffici. L'unità amministrativa responsabile (dipartimento o CaF) comunica i risultati della VIPD, in particolare nella proposta al Consiglio federale, nel rapporto esplicativo, nel messaggio e nelle spiegazioni di voto del Consiglio federale.

## 3 Contenuto della VIPD

### 3.1 Osservazioni preliminari: fondamenti della VIPD e metodologia

Secondo l'articolo 22 capoverso 3 LPD, «la valutazione d'impatto sulla protezione dei dati contiene una descrizione del trattamento previsto, una valutazione dei rischi per la personalità o per i diritti fondamentali della persona interessata nonché i provvedimenti a loro tutela».

Inoltre il numero 3 capoverso 1 delle direttive VIPD precisa che «la VIPD comprende le fasi seguenti:

a. descrizione del trattamento previsto;
b. valutazione dei rischi per i diritti fondamentali della persona interessata;
c. identificazione delle misure previste a tutela dei diritti fondamentali;

[10] RS **235.11**.

[11] RS **152.3**.

[12] Cfr. n 3.7 sui i risultati della VIPD.

d. valutazione degli effetti delle misure previste, per determinare se permane un rischio residuo elevato».

La VIPD dell'unita amministrativa responsabile deve vertere almeno sui quattro punti citati.

**Coordinamento con il metodo di gestione dei progetti HERMES (n. 5 direttive VIPD):** alcune parti della VIPD sono effettuate nel quadro di HERMES; sono ad esempio parte integrante della VIPD l'analisi delle basi legali e gli strumenti allestiti in caso di bisogno di protezione elevato[13].

### 3.2 Indicazioni generali

Le indicazioni generali della VIPD contengono essenzialmente gli stessi elementi che figurano nell'omonima rubrica dello strumento per l'esame preliminare dei rischi.

Devono contenere in particolare le informazioni sull'unità amministrativa responsabile e sulla persona di contatto in seno a questa unità.

Devono indicare anche le basi legali esistenti o previste per il trattamento, al fine di determinare se e quali basi legali è necessario creare o adeguare.[14] L'unità amministrativa responsabile deve eventualmente confrontare le basi legali esistenti con quelle previste.

**Coordinamento con il metodo di gestione dei progetti HERMES (n. 5 direttive VIPD):** nel quadro di HERMES, le indicazioni sulle basi legali esistenti e previste possono essere riprese dall'analisi delle basi legali, purché ancora attuale.

In questa parte è anche indicata anche l'identità del consulente per la protezione dei dati e preciserà se tale persona è stata consultata nel quadro della VIPD.

**Coordinamento con la procedura legislativa (n. 4 direttive VIPD):** l'unità amministrativa deve indicare se la VIPD è effettuata nel quadro di una procedura legislativa, in particolare di una revisione di ordinanza o di legge. Al coordinamento con la procedura legislativa si applicano le direttive del Consiglio federale per l'esame preliminare dei rischi e la valutazione d'impatto sulla protezione dei dati in caso di trattamento di dati personali da parte dell'Amministrazione federale.

**Coordinamento con il metodo di gestione dei progetti HERMES (n. 5 direttive VIPD):** va indicato se la VIPD è effettuata nel quadro di HERMES. Il coordinamento con HERMES è disciplinato dalle direttive del Consiglio federale per l'esame preliminare dei rischi e la valutazione d'impatto sulla protezione dei dati in caso di trattamento di dati personali da parte dell'Amministrazione federale.

[13] www.ncsc.admin.ch > Documentazione > Direttive sulla sicurezza TIC > Procedura di sicurezza > Protezione elevata.

[14] È possibile eseguire l'analisi nel quadro del metodo HERMES: www.hermes.admin.ch/it/.

**Panoramica delle indicazioni generali**

| | |
|---|---|
| Unità amministrativa responsabile | |
| Persona di contatto (cognome, nome, numero telefonico, e-mail) | |
| Basi legali esistenti o previste | |
| Consulente per la protezione dei dati (cognome, nome, numero telefonico, e-mail) | |
| Coordinamento con la procedura legislativa | Sì ☐ No ☐ |
| Applicazione di HERMES | Sì ☐ No ☐ |

### 3.3 Descrizione del trattamento previsto

Occorre innanzitutto descrivere il trattamento previsto (art. 22 cpv. 3 LPD). In linea generale, tale descrizione nella VIPD verte sugli stessi elementi che figurano nella seconda parte dello strumento per l'esame preliminare dei rischi («indicazioni sul trattamento»).

Comprende il tipo, l'entità, lo scopo e le circostanze del trattamento (art. 22 cpv. 2 LPD). L'unità amministrativa responsabile illustra chi tratterà i dati, per quale scopo e come. Nell'ampliare e sviluppare i sistemi e le applicazioni esistenti, la descrizione del trattamento previsto deve contenere anche un confronto con quello attuale.

La descrizione dettagliata del trattamento previsto costituisce la base per la successiva valutazione dei rischi (cfr. n. 3.4). In caso di rischio per la sicurezza delle informazioni, ad esempio, il trattamento previsto può avere un impatto più grave sulla persona interessata se si tratta di dati degni di particolare protezione.

L'unità amministrativa responsabile deve precisare chi tratterà i dati. In particolare occorre indicare se sono presenti più titolari del trattamento[15] o se s'intende incaricare un responsabile del trattamento[16].

Occorre inoltre definire il tipo di dati trattato. Per le categorie dei dati va indicato in particolare se e in che misura il trattamento concerne dati personali[17] e dati personali degni di protezione[18] . È necessario indicare anche la forma dei dati (p. es. testo, audio, video) e le categorie delle persone interessate (p. es. impiegati, assicurati). Se il trattamento include dati di persone vulnerabili (p. es. persone affette da disabilità fisica o psichica, minori, anziani), occorre tenerne conto e valutare se è necessaria una protezione particolare.

Le indicazioni comprendono anche una descrizione del tipo di trattamento. In tal caso l'unità amministrativa responsabile comunica il tipo di trattamento che intende eseguire e la modalità di esecuzione. Tali informazioni vertono sui seguenti tipi di trattamento: raccolta, registrazione, conservazione, utilizzazione, modificazione, comunicazione, archiviazione, cancellazione o

[15] Art. 5 lett. j LPD definisce il concetto di titolare del trattamento.

[16] Art. 5 lett. k LPD definisce il concetto di responsabile del trattamento.

[17] Art. 5 lett. a LPD definisce il concetto di dati personali.

[18] Art. 5 lett. c LPD elenca i dati personali degni di particolare protezione. Per gli esempi consultare lo strumento per l'esame preliminare dei rischi.

distruzione di dati[19]. Va ad esempio indicato se i dati personali sono raccolti di nascosto (ossia all'insaputa della persona interessata)[20], se sono raggruppati o confrontati con dati di altre banche dati[21] nonché se e come vengono trasmessi a terzi (p. es. tramite accesso online[22] o comunicazione all'estero[23]). Dalla descrizione si deve poter evincere se è prevista una profilazione o una profilazione a rischio elevato[24] o se saranno prese decisioni individuali automatizzate[25] . L'unità amministrativa deve indicare se il trattamento include una sorveglianza di persone[26].

Occorre descrivere come verrà attuato il trattamento di dati sotto il profilo tecnico (p. es. software, rete) e con quali tecnologie. È necessario inoltre valutare se il trattamento dei dati si basa su nuove tecnologie o su tecnologie che, pur non essendo nuove, comportano dei rischi per i diritti fondamentali delle persone interessate, con un impatto che non può essere valutato; l'intelligenza artificiale ne è un esempio[27].

È opportuno poi determinare l'entità del trattamento. Le indicazioni devono rivelare se è trattata una grande quantità di dati, se è interessato un gran numero di persone e se il trattamento è esteso dal punto di vista temporale o geografico[28]. In termini temporali occorre indicare la durata del trattamento e della conservazione dei dati personali. Per stabilire se il trattamento è di vasta portata, si può considerare se il trattamento di dati personali costituisce l'attività principale dell'unità amministrativa responsabile. Tale criterio non è tuttavia determinante in sé, ma va considerato insieme ad altri criteri per desumere la presenza o meno di un trattamento di vasta portata[29].

La descrizione deve inoltre contenere lo scopo della raccolta e del trattamento dei dati personali.

### 3.4 Valutazione dei rischi per i diritti fondamentali della persona interessata

In linea generale, questa parte della VIPD richiama la terza parte dello strumento per l'esame preliminare dei rischi («valutazione del rischio elevato»). Seppur utili, tali indicazioni non sono però sufficienti. Nella VIPD occorre infatti identificare i rischi determinando per ciascuno la probabilità che si verifichi come anche l'impatto del rischio per i diritti fondamentali della persona interessata. Per quanto riguarda la gravità, ovvero l'impatto del rischio sui diritti fondamentali della persona interessata, possono costituire un indizio i fattori di rischio identificati nello strumento per l'esame preliminare dei rischi.

---

19 Art. 5 lett. d LPD.

20 Per gli esempi consultare lo strumento per l'esame preliminare dei rischi.

21 Per gli esempi consultare lo strumento per l'esame preliminare dei rischi.

22 L'accesso online costituisce una forma di comunicazione specifica. Il destinatario può accedere ai dati personali in maniera autonoma, senza l'intervento del titolare del trattamento (principio del self-service).

23 Art. 16-18 LPD.

24 Art. 5 lett. f e g definiscono il concetto di profilazione e profilazione a rischio elevato. Per gli esempi consultare lo strumento per l'esame preliminare dei rischi.

25 Art. 21 cpv. 1 LPD definisce il concetto di decisione individuale automatizzata. Per gli esempi consultare lo strumento per l'esame preliminare dei rischi.

26 Per gli esempi consultare lo strumento per l'esame preliminare dei rischi.

27 Per ulteriori esempi consultare lo strumento per l'esame preliminare dei rischi.

28 Per gli esempi consultare lo strumento per l'esame preliminare dei rischi.

29 Per gli esempi consultare lo strumento per l'esame preliminare dei rischi.

### 3.4.1 Identificazione dei rischi

La nozione di rischio rimanda a un possibile evento che ha o può avere ripercussioni sui diritti fondamentali della persona interessata. La valutazione dei rischi determina la probabilità con cui un rischio può verificarsi e l'impatto che ha o può avere per la persona interessata. Occorre anzitutto identificare i possibili rischi del trattamento dei dati personali previsto.

Esistono diversi tipi di rischio. **I rischi per la sicurezza delle informazioni** sono legati alla sicurezza dei dati.

Esempi (cfr. anche l'elenco nella dettagliata analisi dei rischi del piano SIPD[30]):

- violazione dell'integrità dei dati personali, ad esempio a causa di manipolazione o errori di sistema;
- violazione della confidenzialità, ad esempio a causa di vulnerabilità del sistema, uso improprio delle informazioni o attacco al sistema;
- violazione della disponibilità, ad esempio a causa di guasti al sistema, perdita delle informazioni o ransomware;
- violazione della tracciabilità, ad esempio a causa di falsificazione o perdita dei protocolli.

I **rischi per la protezione dei dati** si riferiscono alle singole attività di trattamento, esulando dalla sicurezza dei dati.

Esempi:

- raccolta e trattamento illeciti di dati personali;
- uso di dati personali per scopi non previsti;
- trattamento di dati non corretti;
- accesso non autorizzato ai dati personali;
- eccessiva conservazione dei dati personali;
- diniego dei diritti delle persone interessate.

L'identificazione dei rischi dipende dalle circostanze del caso. Per ogni trattamento previsto occorre quindi analizzare i rischi che sussistono o potrebbero sussistere e determinare i possibili scenari. L'accesso non autorizzato ai dati personali potrebbe ad esempio verificarsi se i collaboratori interni accedono a dati personali che non sono necessari per l'adempimento delle loro mansioni. È anche ipotizzabile che esterni riescano ad accedere illegalmente ai dati personali (p. es. nel quadro di un attacco hacker; cfr. la tabella al n. 3.4.2).

Nell'identificare i rischi è importante definirli in modo rilevante per la protezione dei dati personali. Non vanno indicati rischi astratti che influiscono solo indirettamente sulla protezione dei dati personali (p. es. terremoto).

Le misure previste sono irrilevanti nell'identificare i possibili rischi. L'accesso ai dati non va ad esempio disciplinato in tale sede, ma entra in gioco qualora dalla valutazione dei rischi dovesse emergere la necessità di misure volte a impedire accessi non autorizzati.

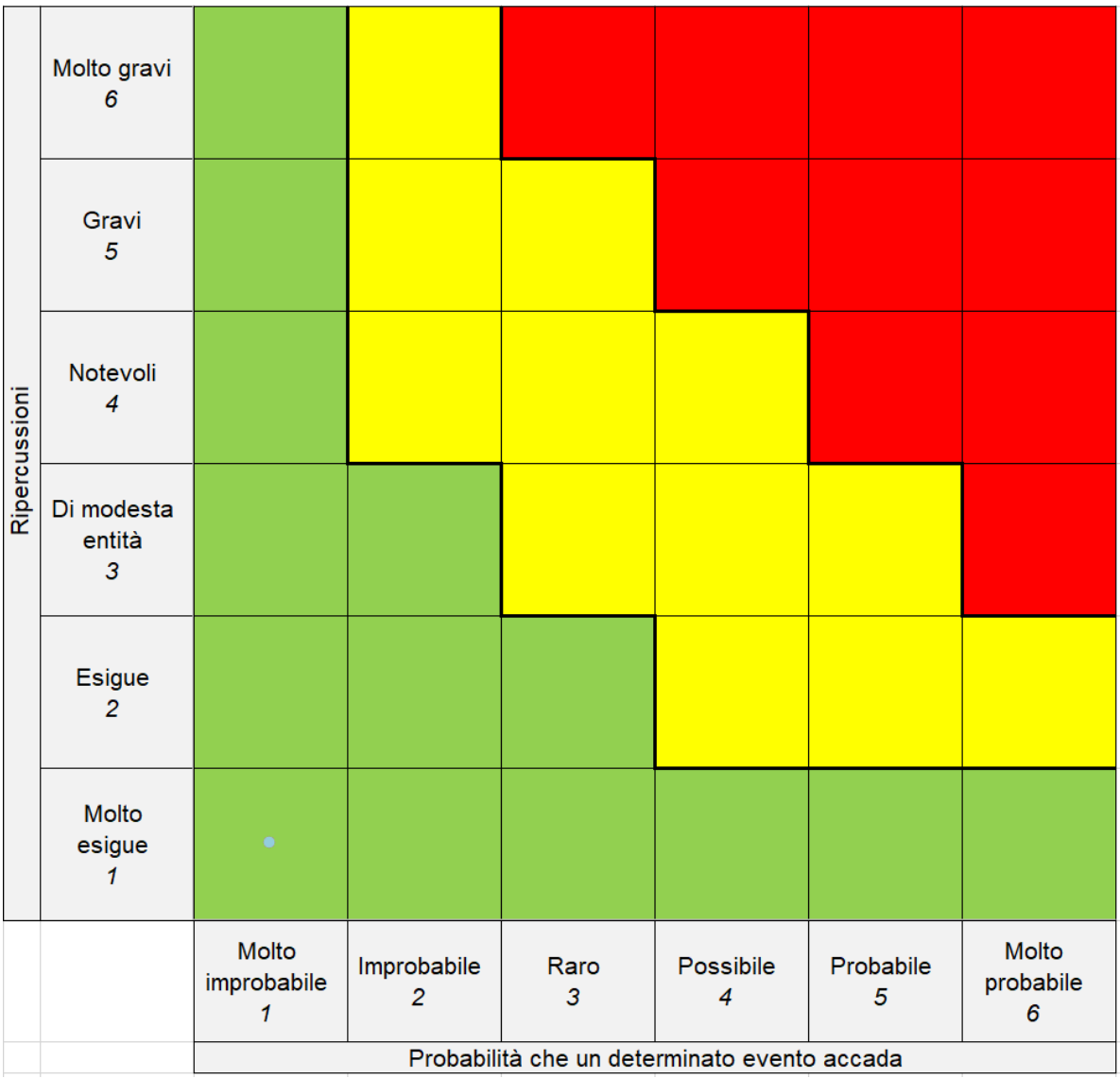
[30] Il modello per l'analisi del rischio nel quadro del piano SIPD è reperibile al seguente indirizzo: www.ncsc.admin.ch > Documentazione > Direttive sulla sicurezza TIC > Procedura di sicurezza > Protezione elevata.

**<u>Coordinamento con il metodo di gestione del progetto HERMES (n. 5 Direttive VIPD)</u>**: se dall'analisi del bisogno di protezione risulta un bisogno di protezione elevato, occorre redigere una dettagliata analisi dei rischi nel quadro del piano SIPD, corredata da identificazione e valutazione dei rischi per la sicurezza delle informazioni. Il piano SIPD è parte integrante della VIPD. I rischi per la protezione dei dati vanno identificati e valutati in maniera separata o nel quadro del piano SIPD.

### 3.4.2 Valutazione dei rischi

In tale quadro viene valutata la probabilità con cui si verificano i rischi identificati e le ripercussioni che hanno o potrebbero avere sui diritti fondamentali della persona interessata.

È possibile valutare i rischi con l'aiuto della matrice dei rischi (metodo 6x6), applicata anche nel quadro dell'analisi dettagliata dei rischi.[31]




[31] Il modello per l'analisi del rischio nel quadro del piano SIPD è reperibile al seguente indirizzo: www.ncsc.admin.ch > Documentazione > Direttive sulla sicurezza TIC > Procedura di sicurezza > Protezione elevata.

Le ripercussioni possono essere di natura fisica (p. es. un trattamento medico errato a causa di dati inesatti), materiale (p. es. perdita del posto di lavoro, uso improprio di carte di credito, riscossione ingiustificata di emolumenti) o immateriale (p. es. discriminazioni, quali razzismo, sessismo, svantaggi sociali, stigmatizzazione per malattia). Le ripercussioni sui diritti fondamentali dell'interessato o la gravità dei rischi possono essere suddivisi in sei livelli: molto esigue, esigue, di modesta entità, notevoli, gravi, molto gravi, definiti come segue.

- Molto esigue: nessuna ripercussione sui diritti fondamentali, nessuna lesione rilevante sotto il profilo morale e sociale, nessun danno finanziario con nesso causale adeguato. Esempi: superamento minimo della durata di conservazione dei dati personali consentita; chiamate telefoniche o messaggi indesiderati senza conseguenza diretta e indiretta.
- Esigue: ripercussione trascurabile sui diritti fondamentali, lesione appena rilevante sotto il profilo morale e sociale, minimo danno finanziario con nesso causale adeguato. Esempio: necessità di cambiare i propri dati di accesso, l'indirizzo e-mail o il numero di telefono.
- Di modesta entità: ripercussione sui diritti fondamentali lieve a lungo termine o grave a breve termine, piccola lesione sotto il profilo fisico, morale e sociale, danno finanziario con nesso causale adeguato. Esempio: acquisto influenzato in maniera scorretta e inammissibile.
- Notevoli o gravi[32]: grave ripercussione a lungo termine sui diritti fondamentali, lesioni medio gravi sotto il profilo fisico, psichico, morale o sociale, importante danno finanziario con nesso causale adeguato. Esempi: rifiuto/scioglimento di un rapporto contrattuale; danno alla reputazione.
- Molto gravi: fatale ripercussione sui diritti fondamentali, grave lesione sotto il profilo fisico, psichico, morale o sociale, danno finanziario con nesso causale adeguato, la cui gravità minaccia l'esistenza. Esempi: trattamento medico erroneo a causa di informazioni inesatte o identificazione errata dei pazienti; rischio di repressione transnazionale in seguito alla divulgazione allo Stato di origine di dati personali dei richiedenti l'asilo, con ripercussioni per la persona interessata o la sua famiglia (integrità fisica, vita, ecc.).

La probabilità di accadimento è una stima della probabilità che un certo evento si verifichi in un certo periodo di tempo nel futuro. La probabilità che accada un determinato evento può essere classificata come: molto improbabile, improbabile, raro, possibile, probabile, molto probabile. La probabilità di occorrenza può essere valutata ricorrendo alle indicazioni applicate nel quadro dell'analisi dei rischi del piano SIPD[33], ossia:

- molto improbabile (oltre 10 anni)
- improbabile (ogni 5-10 anni)
- raro (ogni 3-5 anni)
- possibile (ogni 2-3 anni)
- probabile (ogni 1-2 anni)
- molto probabile (più volte l'anno)

Nel valutare i rischi, è difficile ottenere una stima attendibile. Da un lato vi è la difficoltà di individuare in anticipo la probabilità di occorrenza, poiché non è prevedibile se e quando un rischio si verificherà; dall'altro è difficile stimare le ripercussioni di un rischio. In caso di accesso non autorizzato, può rivelarsi difficile prevedere cosa accadrà ai dati personali e quali ripercussioni si avranno sui diritti fondamentali della persona interessata. Malgrado queste difficoltà, è comunque

[32] La sfumatura tra le due categorie è difficile da definire e dipende dal singolo caso.

[33] Il modello per l'analisi del rischio nel quadro del piano SIPD è reperibile al seguente indirizzo: www.ncsc.admin.ch > Documentazione > Direttive sulla sicurezza TIC > Procedura di sicurezza > Protezione elevata.

importante tentare di definire al meglio i possibili rischi, al fine di poter concepire, in un secondo momento, misure in grado di proteggere al meglio i diritti fondamentali delle persone interessate.

I rischi che nella matrice appaiono verdi possono essere considerati accettabili; vale a dire che i rischi residui possono essere accettati senza dover prevedere misure. I rischi che appaiono gialli o rossi sono da considerarsi elevati ed è necessario adottare misure che li riportino nella zona verde.

**In caso di applicazione di HERMES (cfr. n. 3.4.1)**: poiché i rischi per la sicurezza delle informazioni sono già identificati e valutati nella dettagliata analisi dei rischi (piano SIPD), in questa sede basta identificare e valutare i rischi per la protezione dei dati, in maniera separata o nel quadro del piano SIPD. Riguardo ai rischi per la sicurezza delle informazioni, occorre inoltre garantire che siano valutati anche le ripercussioni sui diritti fondamentali della persona interessata.

**Esempio** (astratto, da concretare per il caso specifico):

| Scenario | Rischio | Probabilità che un evento accada | Ripercussioni per la persona interessata |
|---|---|---|---|
| Accesso interno: diverse persone coinvolte nel trattamento dei dati personali | Accesso non autorizzato ai dati personali | Interno: difficile da determinare. È possibile presumere un comportamento conforme al diritto? Il personale è già sensibilizzato/formato sui rischi? Considerare il comportamento precedente | Interno/esterno: dati personali pervenuti a persone non autorizzate; diverse ripercussioni a seconda del tipo di dati personali e dell'interesse per i dati personali (p. es. uso improprio di carte di credito, utilizzo dei dati, come indirizzo e-mail, da parte di terzi ecc.) |
| Accesso esterno: scarsa sicurezza del sistema (hackeraggio ecc.) | | Esterno: in funzione dell'interesse per i dati personali | |

### 3.5 Identificazione delle misure previste a tutela dei diritti fondamentali

Dopo aver identificato il rischio o i rischi per i diritti fondamentali della persona interessata, è possibile prevedere determinate misure per ridurre tali rischi e proteggere i diritti fondamentali. Contrariamente ai capitoli precedenti, la parte della VIPD relativa all'identificazione delle misure a tutela dei diritti fondamentali non è contemplata dallo strumento per l'esame preliminare dei rischi, che non tiene conto delle misure capaci di ridurre i rischi.

L'identificazione delle misure mira in particolare a ridurre al minimo i rischi per i diritti fondamentali dell'interessato. Le misure previste devono garantire che il rischio netto (stimato considerando tali misure) sia inferiore al rischio lordo (senza misure). La VIPD serve anche a rendere trasparenti i rischi individuati e le relative misure previste.

È possibile ridurre il rischio intervenendo sia sulla probabilità di occorrenza, sia sulla gravità dell'evento scatenante, ossia l'impatto del rischio.

Le misure possono essere di natura tecnica (in pratica si tratta spesso di provvedimenti informatici), organizzativa (in particolare sul piano del personale; ripartizione dei ruoli e delle responsabilità; istruzioni, sorveglianza, ecc.) e/o giuridiche (adozione di basi legali, direttive, regolamenti, contratti, ecc.).

Una serie di misure, in particolare di ordine tecnico e organizzativo, figurano nella LPD e l'OPDa, come ad esempio le norme di sicurezza dei dati, l'obbligo di stilare un regolamento per il trattamento e di tenere un registro delle attività di trattamento, la limitazione e la durata di conservazione, la verifica dell'esattezza dei dati, ecc.

Si tratta d'individuare le misure più opportune per il rischio atteso, il che potrebbe richiedere una certa creatività. Le misure possono vertere direttamente sul trattamento dei dati personali (crittografia, anonimizzazione, pseudonimizzazione, controllo di accesso, tracciabilità, ecc.), il sistema di trattamento (sicurezza del hardware, dei software, verbalizzazione, backup, ecc.) o la governance in materia di protezione dei dati personali (regolamento per il trattamento, gestione dei progetti, del personale o delle violazioni di dati).

In pratica conviene individuare le misure del caso per ridurre i rischi situati nella zona gialla o rossa della matrice. Per ogni misura identificata, occorre inoltre determinare l'attuatore (servizio o funzione), la data di inizio, la durata e il costo (in termini finanziari e di personale).

È possibile presentare tali informazioni sotto forma di tabella:

| **Rischio** | **Misure** | **Servizio/funzione** | **Scadenzario** | **Costi** |
|---|---|---|---|---|
| Rischio 1 | Misura 1 | xy | Da… a… / a partire da… | … |
| | Misura 2 | ef | Da… a… / a partire da… | … |
| | Misura 3 | xy | Da… a… / a partire da… | … |
| Rischio 2 | Misura 2 | ef | Da… a… / a partire da… | … |
| Rischio 3 | Misura 1 | xy | Da… a… /a partire da… | … |
| | Misura 4 | ab | Da… a… / a partire da… | … |

Le misure da adottare nell'ambito della protezione di base andrebbero menzionate nella VIPD se contribuiscono a ridurre il rischio per i diritti fondamentali di una persona. Tuttavia non è necessario indicarne i costi di attuazione.

**In caso di applicazione di HERMES (cfr. n. 3.4.1)**: poiché le misure per i rischi della sicurezza delle informazioni sono già stabilite nella dettagliata analisi del rischio (piano SIPD), in questa sede basta prevedere le misure per i rischi della protezione dei dati, in maniera separata o nel quadro del piano SIPD. Riguardo ai rischi per la sicurezza delle informazioni, è necessario garantire che siano valutate anche le ripercussioni sui diritti fondamentali della persona interessata.

**Esempio** (astratto, da concretare per il caso specifico):

| Scenario | Rischio | Probabilità che un evento accada | Ripercussioni per la persona interessata | Misure |
|---|---|---|---|---|
| Accesso interno: diverse persone coinvolte nel trattamento dei dati personali | Accesso non autorizzato ai dati personali | Interno: difficile da determinare. È possibile presumere un comportamento conforme al diritto? Il personale è già sensibilizzato / formato sui rischi? Considerare il comportamento precedente | Interno/esterno: dati personali pervenuti a persone non autorizzate; diverse ripercussioni a seconda del tipo di dati personali e dell'interesse per i dati personali (p. es. uso improprio di carte di credito, utilizzo dei dati, come indirizzo e-mail, da parte di terzi, ecc.) | Disciplinamento dei diritti d'accesso; verbalizzazione degli accessi; formazione e direttive interne; verifica del rispetto delle direttive |
| Accesso esterno: scarsa sicurezza del sistema (hackeraggio ecc.) | | Esterno: in funzione dell'interesse per i dati personali | | Migliorare la sicurezza del sistema; informare le persone interessate in caso di violazione della protezione dei dati |

### 3.6 Valutazione degli effetti delle misure previste, al fine di determinare l'eventuale presenza di un rischio residuo elevato

Dopo aver determinato le misure, l'unità amministrativa responsabile dovrà procedere a una nuova valutazione di ogni rischio identificato nella zona gialla o rossa della matrice (cfr. n. 3.4), per stabilire se le misure previste hanno permesso di cogliere e ridurre il rischio e per verificare l'eventuale presenza di un rischio residuo elevato (nella zona gialla o rossa della matrice).

Andranno ad esempio valutate le misure tecniche e organizzative previste in materia di sicurezza dei dati per determinare la probabilità e la gravità di una violazione della sicurezza dei dati nonostante le misure adottate.

Da notare che alcuni rischi non sono influenzabili o lo sono solo in parte. Infatti, pur adottando diverse misure, è possibile che il rischio resti invariato o quasi.

Un rischio elevato per i diritti fondamentali della persona interessata nonostante le misure previste non impedisce il trattamento dei dati, ma implica il ricorso all'IFPDT[34]. Prima di trattare i dati, il titolare deve quindi consultare l'IFPDT e tenere conto delle eventuali misure che questi propone terminato il suo esame. L'IFPDT si esprime entro due tre mesi[35].

**Coordinamento con la procedura legislativa (n. 4 direttive VIPD):** i risultati della VIPD e, in caso di rischio residuo elevato ai sensi dell'articolo 23 LPD, il **parere dell'IFPDT** sono allegati all'incarto per la consultazione degli uffici. Se la necessità di effettuare o adeguare una VIPD

[34] Art. 23 LPD.

[35] Art. 23 cpv. 2 LPD.

emerge dopo la consultazione, i risultati ed eventualmente il parere dell'IFPDT sono allegati all'incarto per la seguente consultazione degli uffici o la procedura di corapporto.

L'unità amministrativa responsabile (dipartimento o CaF) comunica i risultati della VIPD ed eventualmente il **parere dell'IFPDT** in particolare nella proposta al Consiglio federale, nel rapporto esplicativo, nel messaggio e nelle spiegazioni di voto del Consiglio federale.

**Esempio** (astratto, da concretare per il caso specifico):

| **Scenario** | **Rischio** | **Probabilità che un evento accada** | **Ripercussioni per la persona interessata** | **Misure** | **Effetti delle misure (rischio residuo)** |
|---|---|---|---|---|---|
| Accesso interno: diverse persone coinvolte nel trattamento dei dati personali | Accesso non autorizzato ai dati personali | Interno: difficile da determinare. È possibile presumere un comportamento conforme al diritto? Il personale è già sensibilizzato / formato sui rischi? Considerare il comportamento precedente | Interno/esterno: dati personali pervenuti a persone non autorizzate; diverse ripercussioni a seconda del tipo di dati personali e dell'interesse per i dati personali (p. es. uso improprio di carte di credito, utilizzo di dati, come indirizzo e-mail, ecc.) | Disciplinamento dei diritti d'accesso; verbalizzazione degli accessi; formazione e direttive interne; verifica del rispetto delle direttive | Misure tecniche e organizzative possono contenere in larga misura la probabilità che un rischio si verifichi; le ripercussioni in caso di evento possono essere arginate solo in maniera limitata |
| Accesso esterno: scarsa sicurezza del sistema (hackeraggio ecc.) | | Esterno: in funzione dell'interesse per i dati personali | | Migliorare la sicurezza del sistema; informare le persone interessate in caso di violazione della protezione dei dati | Una migliore sicurezza del sistema può contenere in larga misura la probabilità che un rischio si verifichi; le ripercussioni in caso di evento possono essere arginate solo in maniera limitata |

### 3.7 Sintesi e risultati della VIPD

La sintesi deve menzionare i risultati principali della VIPD, vale a dire i rischi (situati nella zona gialla o rossa della matrice), le misure previste per ridurre tali rischi e gli eventuali rischi residui elevati.

**Coordinamento con la procedura legislativa (n. 4 direttive VIPD):** i risultati di una VIPD effettuata nel quadro di una procedura legislativa, vanno allegati all'incarto per la consultazione degli uffici. L'unità amministrativa responsabile (dipartimento o CaF) comunica i risultati della VIPD, in particolare nella proposta al Consiglio federale, nel rapporto esplicativo, nel messaggio e nelle spiegazioni di voto del Consiglio federale.

**Allegato: checklist VIPD**

**Prima parte: indicazioni generali**

La prima parte contiene le seguenti indicazioni generali:

☐ Unità amministrativa responsabile.

☐ Basi legali esistenti o previste per il trattamento dei dati personali.

☐ Consulente per la protezione dei dati.

☐ Precisazione che il trattamento previsto si iscrive nel quadro di una procedura legislativa.

☐ Precisazione che il trattamento previsto si iscrive nel quadro di un progetto HERMES.

**Seconda parte: descrizione del trattamento previsto**

La seconda parte descrive il trattamento previsto indicandone il tipo, l'entità, lo scopo e le circostanze.

☐ Identificazione delle persone coinvolte nel trattamento (p. es. diversi titolari e responsabili del trattamento).

☐ Identificazione e descrizione delle categorie di dati personali (p. es. dati personali / degni di particolare protezione, forma dei dati).

☐ Identificazione e descrizione delle categorie degli interessati (p. es. persone vulnerabili).

☐ Identificazione e descrizione del trattamento previsto (p. es. raccolta, registrazione, conservazione, utilizzazione, modificazione, comunicazione, archiviazione, cancellazione o distruzione dei dati).

☐ Identificazione e descrizione del tipo di trattamento (p. es. raccolta di dati personali senza il consenso della persona interessata, unificazione o confronto con altre banche dati, comunicazione di dati personali a terzi, profilazione ad alto rischio, decisione individuale automatizzata, sorveglianza di persone).

☐ Identificazione e descrizione delle tecnologie utilizzate (p. es. software, rete, intelligenza artificiale).

☐ Identificazione e descrizione dell'entità del trattamento (p. es. quantità dei dati personali trattati, numero delle persone interessate, entità temporale e geografica).

☐ Identificazione e descrizione dello scopo del trattamento.

**Terza parte: valutazione dei rischi per i diritti fondamentali della persona interessata**

La terza parte valuta i rischi fondandosi sugli elementi seguenti:

☐ Identificazione e descrizione dei rischi per la sicurezza delle informazioni e la protezione dei dati.

☐ Valutazione della probabilità che i rischi identificati si verifichino.

☐ Valutazione e descrizione delle ripercussioni o della gravità dei rischi per i diritti fondamentali della persona interessata

Per ogni rischio identificato, occorre determinare:

☐ se il rischio è accettabile (zona verde della matrice).

☐ se il rischio non è accettabile (zona gialla o rossa della matrice) → identificare i possibili correttivi; cfr. punto successivo).

**Quarta parte: identificazione delle misure previste a tutela dei diritti fondamentali**

La quarta parte identifica le misure previste a tutela dei diritti fondamentali, ossia quelle che consentono di passare dal rischio lordo a quello netto.

Per ogni rischio identificato nella zona gialla o rossa della matrice (cfr. n. 3.4):

☐ Identificazione delle misure pertinenti volte a ridurre il rischio.

Per ogni misura identificata va indicato:

☐ Il servizio o la persona (funzione) responsabile dell'attuazione della misura.

☐ Lo scadenzario per l'attuazione della misura.

☐ Il costo (in termini finanziari e di personale) dell'attuazione della misura.

Identificazione e valutazione del rispetto:

☐ Dei principi in materia del diritto della protezione dei dati.

☐ Degli obblighi del titolare del trattamento.

**Quinta parte: valutazione degli effetti delle misure previste, al fine di determinare l’eventuale presenza di un rischio residuo elevato**

La quinta parte serve a determinare se, nonostante le misure previste a tutela dei diritti fondamentali, permane un rischio residuo elevato.

Per ogni misura prevista:

☐ Valutazione e descrizione degli effetti delle misure citate.

Per ogni rischio identificato nella zona gialla o rossa della matrice, va determinato:

☐ Se sussiste un rischio residuo elevato.

☐ Se consultare eventualmente l'IFPDT.

**Sesta parte: sintesi e risultati della VIPD**

L’ultima parte presenta una sintesi dei risultati.

☐ Descrizione dei rischi identificati (zona gialla o rossa della matrice).

☐ Descrizione delle misure previste per ridurre tali rischi.

☐ Descrizione degli eventuali rischi residui elevati.