Promemoria sulla valutazione d'impatto sulla protezione dei dati (VIPD)

1. Quando è necessaria una VIPD?

Una VIPD è necessaria quando il trattamento dei dati comporta o può comportare un rischio elevato per la personalità (in caso di trattamento di dati personali degni di particolare protezione o di sorveglianza sistematica di ampi spazi pubblici) o i diritti fondamentali della persona interessata (cfr. art. 22 cpv. 1–3 LPD). L'aspetto decisivo è, segnatamente, se il trattamento dei dati degni di particolare protezione avvenga su scala particolarmente grande o se vengano utilizzate nuove tecnologie.

La VIPD deve contenere almeno 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.

2. Progetto / trattamento dei dati

Innanzitutto va descritto il trattamento dei dati previsto (art. 22 cpv. 3 LPD). Vanno indicate le basi giuridiche vigenti o previste che autorizzano il trattamento. Occorre analizzare se e quali basi giuridiche siano già in vigore oppure debbano essere create o adeguate. Se del caso, le basi giuridiche esistenti vanno confrontate con quelle previste.

3. Descrizione del trattamento dei dati personali previsto

In questo capitolo vanno indicati il tipo, l'entità e lo scopo del trattamento dei dati nonché le circostanze in cui esso viene effettuato (art. 22 cpv. 2 LPD). Lo scopo è il motivo per cui i dati personali vengono raccolti e trattati. Il tipo di trattamento è la descrizione delle operazioni previste, segnatamente la raccolta, la registrazione, la conservazione, l'utilizzazione, la modificazione, la comunicazione, l'archiviazione, la cancellazione o la distruzione di dati.

Al punto concernente la categoria di dati si deve indicare in particolare se e in che misura il trattamento riguardi dati personali o dati personali degni di particolare protezione. Va indicata anche la forma in cui i dati sono disponibili (p. es. forma scritta, registrazione sonora, immagine). Si devono anche descrivere le categorie delle persone interessate (p. es. dipendenti, assicurati).

Dalle indicazioni sull'entità del trattamento risulta se venga trattato un grande volume di dati, se il trattamento interessi un gran numero di persone e se esso sia ampio in termini temporali o geografici. Per quanto riguarda l'aspetto temporale, occorre indicare in particolare per quanto tempo i dati personali verranno trattati e conservati.

4. Analisi dei rischi e misure previste

Identificazione e valutazione dei rischi per i diritti fondamentali della persona interessata
I rischi sono possibili conseguenze negative, non volute, che hanno o possono avere ripercussioni sui diritti fondamentali della persona interessata.

Esempi: perdita di dati, dati non corretti, raccolta eccessiva di dati, accesso non autorizzato ai dati, collegamento di dati o profilazione illeciti, conservazione eccessivamente lunga dei dati, trasmissione dei dati in Stati terzi, forte limitazione della libertà della persona interessata di disporre dei propri dati,

trattamento di una grande quantità di dati, possibilità di accesso ai dati da parte di un elevato numero di persone.

Innanzitutto occorre identificare i potenziali rischi del trattamento di dati personali previsto.

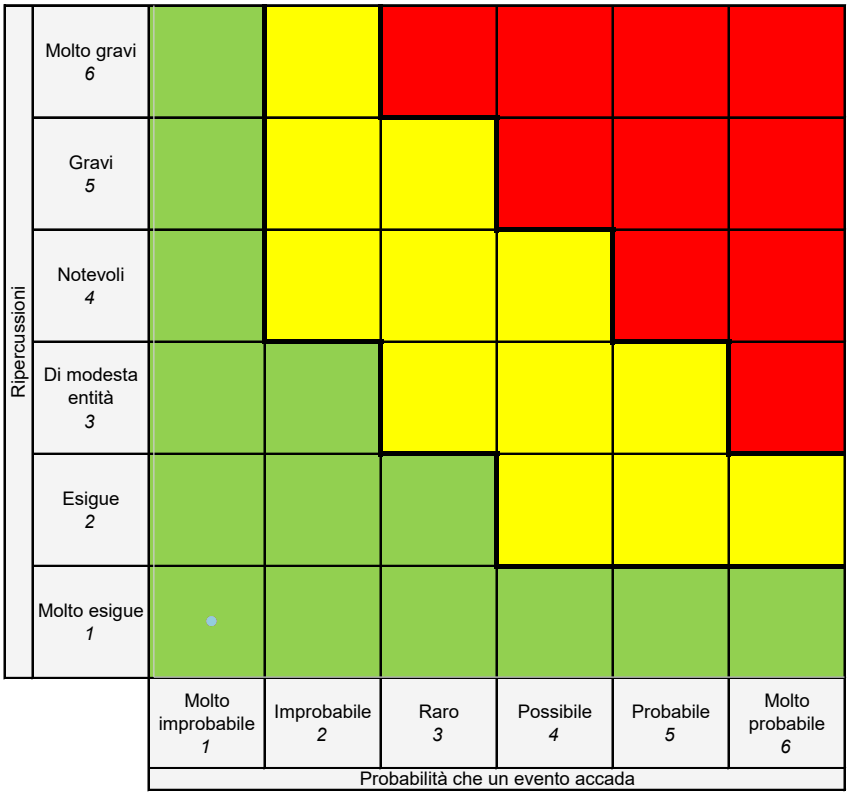
Vi sono diversi tipi di rischi. I rischi per la sicurezza delle informazioni riguardano la sicurezza dei dati. Esempi: violazione dell'integrità dei dati personali, ad esempio a causa di manipolazioni o errori nel sistema; violazione della confidenzialità, ad esempio a causa di vulnerabilità del sistema, uso improprio delle informazioni, attacco al sistema; violazione della disponibilità, ad esempio a causa di guasti ai sistemi, perdita di informazioni o ransomware; violazione della tracciabilità, ad esempio a causa di falsificazione o perdita dei verbali.

I rischi per la protezione dei dati riguardano le singole operazioni di trattamento dei dati e vanno oltre la semplice sicurezza dei dati. Esempi: raccolta o trattamento illeciti di dati personali, utilizzo dei dati personali per scopi non previsti, trattamento di dati non corretti, accesso non autorizzato a dati personali, conservazione eccessivamente lunga dei dati personali, negazione dei diritti della persona interessata.

Probabilità di realizzazione dei rischi

Dopo aver indentificato i potenziali rischi, si devono indicare, per ciascuno di essi, la probabilità della loro realizzazione e le ripercussioni sui diritti fondamentali della persona interessata.

La valutazione dei rischi è effettuata mediante la matrice dei rischi 6x6 applicata anche nell'ambito dell'analisi dettagliata dei rischi del Piano per la sicurezza dell'informazione e la protezione dei dati (piano SIPD)[1]. I rischi figuranti nei campi rossi e gialli della matrice dei rischi sono da considerare quali rischi elevati. Questi rischi devono essere affrontati predisponendo misure adeguate. Queste misure hanno lo scopo di ridurre i rischi.



[1] Il modello per l'analisi dettagliata dei rischi del piano SIPD è disponibile all'indirizzo: https://www.ncsc.admin.ch/ncsc/it/home.html > Documentazione > Direttive sulla sicurezza TIC > Procedura di sicurezza > Protezione elevata.

Le ripercussioni possono essere di natura fisica (p. es. trattamento medico errato a causa di dati non corretti), materiale (p. es. perdita del posto di lavoro, abuso di una carta di credito, addebiti ingiustificati) o immateriale (discriminazione, p. es. razzismo o sessismo; svantaggi sociali; stigmatizzazione dovuta a malattia). Le ripercussioni sui diritti fondamentali della persona interessata o la gravità dei rischi possono essere suddivise in sei livelli: molto esigue, esigue, di modesta entità, notevoli, gravi e molto gravi. I vari livelli sono descritti qui di seguito.

Molto esigue: nessuna ripercussione sui diritti fondamentali; nessun danno morale o sociale percepibile; nessun danno economico con nesso causale adeguato. Esempi: lieve superamento della durata di conservazione dei dati personali, telefonate o messaggi indesiderati senza conseguenze dirette o indirette.

Esigue: ripercussioni trascurabili sui diritti fondamentali; danni morali o sociali quasi impercettibili; eventualmente danni economici minimi con un nesso causale adeguato. Esempi: necessità di cambiare il web account, l'indirizzo e-mail o il numero di telefono.

Di modesta entità: ripercussioni a lungo termine di entità minore o ripercussioni a corto termine di entità grave sui diritti fondamentali; danni psicologici, morali o sociali di entità minore; eventualmente danni economici con un nesso causale adeguato. Esempi: influenza non trasparente e inammissibile sul comportamento in materia di acquisti.

Notevoli/gravi: gravi ripercussioni a lungo termine sui diritti fondamentali; danni fisici, psicologici, morali o sociali di entità medio-grave; danni economici sostanziali con un nesso causale adeguato. Esempi: rifiuto o risoluzione di un rapporto contrattuale; danni alla reputazione.

Molto gravi: ripercussioni fatali sui diritti fondamentali; gravi danni fisici, psicologici, morali o sociali; danni economici con un nesso causale adeguato che minacciano l'esistenza, ad esempio un trattamento medico errato dovuto a informazioni sbagliate sul paziente o sull'identificazione del paziente; rischi legati al perseguimento penale transfrontaliero, ad esempio a causa di una fuga di dati personali dei richiedenti l'asilo che si recano nel loro Paese d'origine; tali rischi riguardano sia la persona interessata che i suoi familiari (integrità fisica, vita ecc.).

La probabilità di realizzazione dei rischi è una stima della probabilità che un determinato evento accada entro un certo intervallo di tempo. Anche questo parametro è suddiviso in sei livelli: molto improbabile, improbabile, raro, possibile, probabile e molto probabile. Per la valutazione della probabilità si può utilizzare la legenda dell'analisi dettagliata dei rischi del piano SIPD, secondo la quale tale probabilità può essere valutata in base ai seguenti criteri:

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 all'anno

Misure previste

Le misure volte a proteggere le persone interessate possono essere di natura sia organizzativa che tecnica.

Esempi di misure organizzative: organizzazione di formazioni, istruzioni, guide per gli utenti, piani di autorizzazione di accesso, obblighi di serbare il segreto, sistemi di gestione della sicurezza delle informazioni (SGSI), processi per i diritti di accesso, processi per le richieste di cancellazione e verifiche di conformità.

Esempi di misure tecniche: controlli d'accesso ai sistemi informatici, controlli d'accesso ai locali, accessi di durata limitata, cifrature, anonimizzazioni e minimizzazioni dei dati.

5. Consultazione del consulente per la protezione dei dati / dell'IFPDT

Se dalla VIPD emerge che, nonostante le misure prese o previste, il trattamento dei dati comporta un rischio elevato per la persona interessata, vanno consultati il consulente per la protezione dei dati e poi l'IFPDT (cfr. art. 10 e art. 23 LPD).