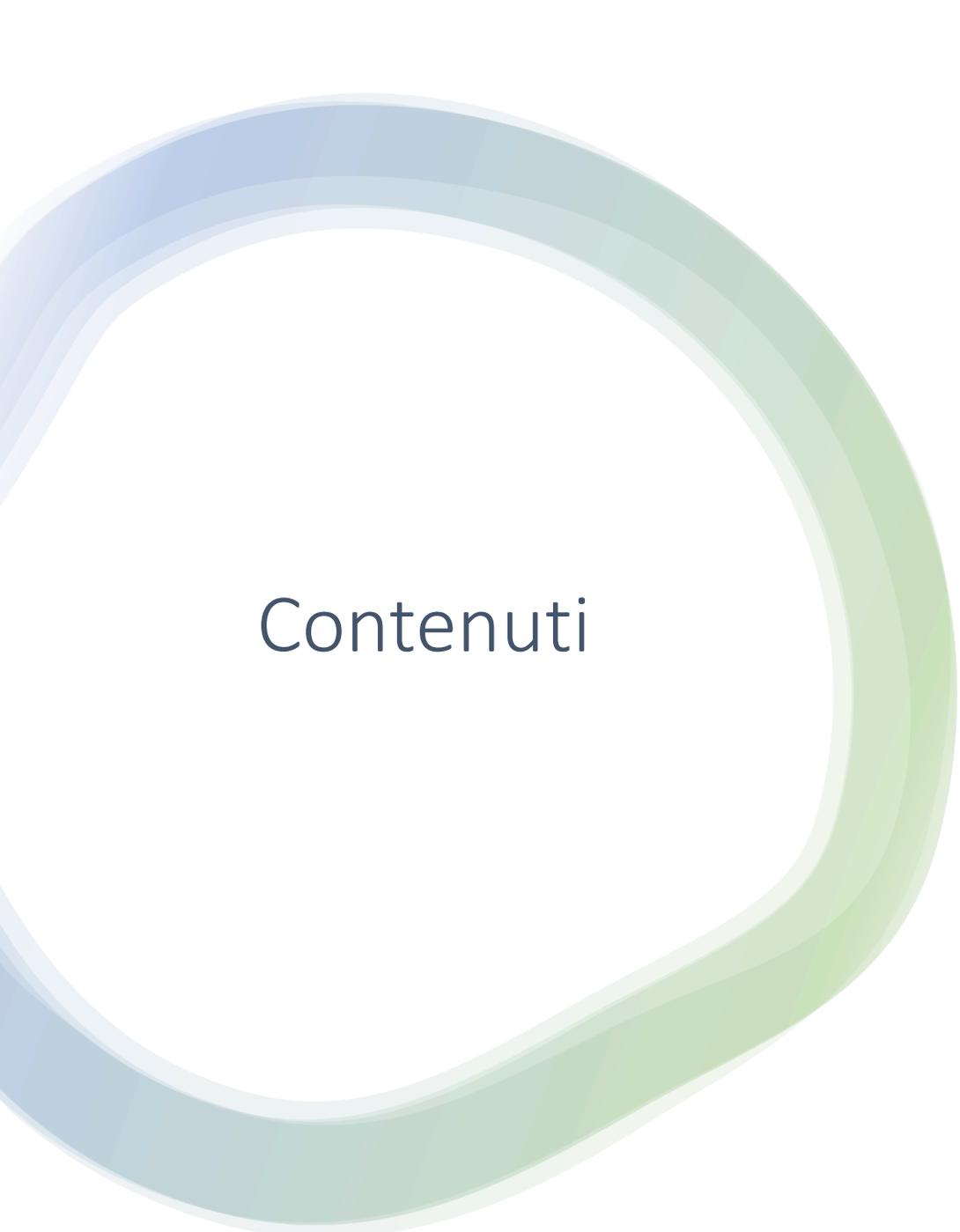


Leggi sulla protezione dei dati

Una breve introduzione

Manno, 5 ottobre 2023





Contenuti

- Breve introduzione diritto in materia di protezione alla LPD (Svizzera), incluse note sulle sanzioni;
- Principi fondamentali delle leggi sulla privacy e strumenti principali;
- Approccio basato sul rischio;
- Piano di risposta agli incidenti informatici; cos'è, perché crearlo.
- Salute e protezione dei dati personali.
- Breve introduzione alla revisione del diritto cantonale.

Breve introduzione al GDPR e alla LPD comprese le note sulle sanzioni.

▶ Che cos'è un dato personale?

▶ GDPR (art. 4)

- ▶ Per 'dati personali' si intende qualsiasi informazione relativa a una persona fisica identificata o identificabile ('soggetto interessato'); una persona fisica identificabile è quella che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificativo come un nome, un numero di identificazione, dati di localizzazione, un identificativo online o a uno o più fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale persona fisica.

▶ Che cos'è un dato personale?

▶ Nuova LPD (ART. 5)

- ▶ a. dati personali: qualsiasi informazione relativa a una persona fisica identificata o identificabile;
- ▶ b. soggetto interessato: persona fisica i cui dati personali vengono elaborati;
- ▶ c. dati personali sensibili:
 - ▶ dati su opinioni o attività religiose, ideologiche, politiche o sindacali,
 - ▶ dati sulla salute, sulla sfera intima o sull'origine razziale o etnica,
 - ▶ dati genetici,
 - ▶ dati biometrici che identificano inequivocabilmente una persona fisica,
 - ▶ dati su procedimenti o sanzioni amministrative e penali,
 - ▶ dati sulle misure di sicurezza sociale;

Breve introduzione al GDPR (Europa) e alla LPD (Svizzera), comprese le note sulle sanzioni.

- ▶ La Nuova Legge Federale sulla Protezione dei Dati (nLPD o nuova LPD) Quali sono i principali cambiamenti?
- ▶ La nLPD ha introdotto i seguenti cambiamenti principali:
 - ▶ Ora sono coperti solo i dati delle persone fisiche e non quelli delle persone giuridiche.
 - ▶ I dati genetici e biometrici rientrano nella definizione di dati sensibili.
 - ▶ Vengono introdotti i principi di "Privacy by Design" e "Privacy by Default".
 - ▶ Le valutazioni d'impatto devono essere condotte se esiste un rischio elevato per la privacy o i diritti fondamentali degli interessati.
 - ▶ L'obbligo di fornire informazioni è stato ampliato: la raccolta di tutti i dati personali - e non più solo dei cosiddetti dati sensibili - richiederà una notifica preventiva alla persona interessata.
 - ▶ La tenuta di un registro delle attività di trattamento è ora obbligatoria. Tuttavia, l'ordinanza prevede delle esenzioni per le PMI il cui trattamento dei dati presenta un rischio limitato di danno per l'interessato.
 - ▶ In caso di violazione della sicurezza dei dati, è necessaria una notifica tempestiva all' Incaricato federale per la protezione dei dati (IFPDT).
 - ▶ Il concetto di profilazione (cioè il trattamento automatizzato dei dati personali) è ora parte della legge.

Breve introduzione al GDPR e al LPD (svizzero), comprese le note sulle sanzioni.

▶ PROCESSO CONSENTITO GDPR:

- ▶ Devono essere rispettati i principi di base del trattamento
 - ▶ Trasparenza, limitazione dello scopo, equità, minimizzazione dei dati, limitazione dell'archiviazione, correttezza, sicurezza dei dati.
- ▶ È necessaria una base legale
- ▶ Contratto, obbligo legale, consenso, interesse legittimo, ecc.
- ▶ Entrato in vigore nel maggio 2018

▶ PROCESSO PERMESSO Nuova LPD:

- ▶ Stessi principi di elaborazione di base
- ▶ Non è richiesta alcuna base legale per impostazione predefinita
 - ▶ Un motivo legale è necessario solo se i principi non vengono rispettati, se i dati sensibili vengono divulgati a terzi o se la persona interessata si oppone.
- ▶ La LPD è meno severa sui motivi legali per i dati personali sensibili.
- ▶ Entrata in vigore il 1° settembre 2023

Breve introduzione al GDPR e al LPD (Svizzera), comprese le note sulle sanzioni.

- ▶ Nuova LPD:

- ▶ Stessa definizione di dati personali (le persone giuridiche non sono più coperte)
- ▶ Qualsiasi trattamento automatizzato o manuale dei dati personali
- ▶ Eccezione per il trattamento a fini personali
- ▶ Non applicabile nei procedimenti legali
- ▶ Applicabile se le attività rilevanti, gli interessati, il responsabile del trattamento o l'incaricato del trattamento si trovano in Svizzera.

Breve introduzione al GDPR e al DPA (Svizzera), comprese le note sulle sanzioni.

▶ GDPR:

- ▶ Dati su persone identificate o identificabili;
- ▶ Applicabilità al di fuori dell'UE (se le persone sono mirate o tracciate nell'UE)
- ▶ Principi di trattamento (trasparenza, limitazione dello scopo, equità, minimizzazione dei dati, limitazione della conservazione, correttezza, sicurezza dei dati);
- ▶ Motivo legale (obbligo legale, contratto, interesse legittimo, consenso);
- ▶ Obblighi di informazione (quasi nessuna eccezione);
- ▶ Diritti individuali (di accesso, di rettifica, di cancellazione/dimenticanza, di restrizione, di opposizione, di portabilità dei dati, di notifica a terzi dell'esercizio di tali diritti).

- **MULTE E SANZIONI**

- ▶ **GDPR**

- Le autorità per la protezione dei dati possono :

- ▶ Indagare sulle attività di elaborazione
 - ▶ Emettere ordini per limitare, modificare o interrompere le attività di trattamento.
 - ▶ Emette multe fino a 10/20 milioni di euro o al 2/4% del fatturato annuale per la violazione della maggior parte delle disposizioni del GDPR.
 - ▶ La legge locale può prevedere multe aggiuntive

- ▶ **Nuova LPD**

- L'autorità per la protezione dei dati può:

- ▶ Indagare sulle attività di elaborazione
 - ▶ Emettere ordini per limitare, modificare o interrompere le attività di trattamento.
 - ▶ Le autorità cantonali possono
 - ▶ Emette multe contro le persone fino a 250'000 franchi svizzeri in caso di violazione intenzionale di alcune disposizioni della LPD o di mancata collaborazione con l'autorità di protezione dei dati.

(nuova) Legge federale sulla protezione dei dati
nLPD, disposizioni penali

Capitolo 8: Disposizioni penali

- Art. 60 Violazione degli obblighi di informare, di concedere l'accesso e di collaborare
- Art. 61 Violazione degli obblighi di diligenza
- Art. 62 Violazione dell'obbligo del segreto
- Art. 63 Inosservanza di decisioni
- Art. 64 Infrazioni commesse nell'azienda
- Art. 65 Competenza
- Art. 66 Prescrizione dell'azione penale

(nuova) Legge federale sulla protezione dei dati
nLPD, disposizioni penali

Art. 60 Violazione degli obblighi di informare, di concedere l'accesso e di collaborare

¹ Sono puniti, a querela di parte, con la multa fino a 250 000 franchi i privati che:

a. violano gli obblighi di cui agli articoli 19, 21 e 25–27, fornendo **intenzionalmente** informazioni inesatte o incomplete;

b. **omettono intenzionalmente**:

1. di informare la persona interessata conformemente agli articoli 19 capoverso 1 e 21 capoverso 1, o

2. di fornire alla persona interessata le informazioni di cui all'articolo 19 capoverso 2.

² Sono puniti con la multa fino a 250 000 franchi i privati che in violazione dell'articolo 49 capoverso 3 **forniscono intenzionalmente all'IFPDT**, nel quadro di un'inchiesta, informazioni false o rifiutano intenzionalmente di collaborare.

(nuova) Legge federale sulla protezione dei dati
nLPD, disposizioni penali

Art. 61 Violazione degli obblighi di diligenza

A querela di parte sono puniti con la multa fino a 250 000 franchi i privati che intenzionalmente:

- a. comunicano dati personali all'estero in violazione dell'articolo 16 capoversi 1 e 2 e senza che sussistano le condizioni di cui all'articolo 17;
- b. affidano il trattamento di dati personali a un responsabile senza che sussistano le condizioni di cui **all'articolo 9 capoversi 1 e 2;**
- c. non rispettano i **requisiti minimi in materia di sicurezza dei dati emanati dal Consiglio** federale in virtù dell'articolo 8 capoverso 3.

(nuova) Legge federale sulla protezione dei dati nLPD, disposizioni penali (art. 62 idc art. 9 nLPD)

Art. 9 Trattamento di dati personali da parte di un responsabile

¹ Il trattamento di dati personali può essere affidato a un responsabile del trattamento per contratto o per legge se:

a. questi effettua soltanto i trattamenti che il titolare del trattamento avrebbe il diritto di effettuare; e

b. nessun obbligo legale o contrattuale di serbare il segreto lo vieta.

² Il titolare del trattamento deve in particolare assicurare che il responsabile del trattamento sia in grado di garantire la sicurezza dei dati.

(nuova) Legge federale sulla protezione dei dati
nLPD, disposizioni penali

Art. 62 Violazione dell'obbligo del segreto

¹ Chiunque **rivela intenzionalmente** dati personali segreti dei quali è venuto a conoscenza nell'esercizio di una professione che richiede la conoscenza di tali dati, è punito, a querela di parte, con la multa fino a 250 000 franchi.

² È passibile della stessa pena **chiunque intenzionalmente** rivela dati personali segreti dei quali è venuto a conoscenza nell'ambito dell'attività svolta per conto della persona sottostante all'obbligo del segreto o in occasione della sua formazione presso tale persona.

³ La rivelazione di dati personali segreti è punibile anche dopo la cessazione dei rapporti di lavoro o della formazione.

(nuova) Legge federale sulla protezione dei dati
nLPD, disposizioni penali

Art. 63 Inosservanza di decisioni

È punito con la multa fino a 250 000 franchi il privato che **intenzionalmente non ottempera a una decisione dell'IFPDT**, o a una decisione delle autorità di ricorso, notificatagli sotto comminatoria della pena prevista nel presente articolo.

(nuova) Legge federale sulla protezione dei dati
nLPD, disposizioni penali

Art. 64 Infrazioni commesse nell'azienda

¹ Alle infrazioni commesse nell'azienda sono applicabili gli articoli 6 e 7 della legge federale del 22 marzo 1974¹⁶ sul diritto penale amministrativo (DPA).

² Se la multa applicabile non supera i 50 000 franchi e se la determinazione delle persone punibili secondo l'articolo 6 DPA esige provvedimenti d'inchiesta sproporzionati all'entità della pena, l'autorità può prescindere da un procedimento contro dette persone e, in loro vece, condannare al pagamento della multa l'azienda (art. 7 DPA).

(nuova) Legge federale sulla protezione dei dati
nLPD, disposizioni penali

Art. 65 Competenza

¹ Il perseguimento e il giudizio dei reati **competono ai Cantoni**.

² **L'IFPDT può sporgere denuncia** presso l'autorità di perseguimento penale competente e avvalersi nel procedimento dei diritti dell'accusatore privato.

Art. 66 Prescrizione dell'azione penale

L'azione penale si prescrive in **cinque anni**.

I principi cardine della nuova LPD posso essere riassunti come segue.

- *Tratta i dati personali sempre lecitamente, secondo la buona fede e il principio della proporzionalità;*
- *Non trattare i dati personali in segreto;*
- *Informa gli interessati in modo chiaro e trasparente dello scopo del trattamento dei dati personali;*
- *Utilizza solo i dati personali che ti servono per raggiungere lo scopo dichiarato;*
- *Definisci scopo e modalità prima di iniziare il trattamento dei dati personali;*
- *Assicurati che i dati personali siano corretti durante il trattamento dei medesimi;*
- *Garantisce la sicurezza dei dati personali, adotta le misure tecniche e organizzative necessarie sin dal principio;*
- *Cancello i dati che non ti servono più a meno che tu non sia tenuto per legge a conservarli o non abbia un interesse legittimo per la loro conservazione.*

Oltre la LPD: leggi federali, cantonali e internazionali che possono tornare applicabili



CP (Codice penale) art. 321, segreto professionale (pena detentiva sino a 3 anni o sanzione pecuniaria)



Legge cantonale sulla protezione di dati personali (LPDP, in fase di revisione, vedi anche STE108 II);



LPD Attuale (art. 35 cpv. 1 multa fino a CHF 10'000.-) e futura (multa fino a CHF 250'000.-)



Codice delle obbligazioni e Codice civile (eventuali procedure civili, anche in materia di tutela delle personalità ex art. 28 e segg. CC);



RGDP ("GDPR") se sono dati i presupposti (multe fino a 10 o 20 mio EUR o 4% fatturato globale del gruppo);



...

Revisione totale LPDP

«Peculiarmente ai diritti delle persone, sono previste le seguenti modifiche:

- ***principio della trasparenza:** il titolare dell'elaborazione è tenuto a fornire all'interessato informazioni di dettaglio relative all'elaborazione di dati che lo concernono; l'informativa deve essere facilmente accessibile e di facile comprensione, in particolar modo nel caso di informazioni a minori;*
- ***diritto di accesso:** sono ampliate le categorie d'informazioni riguardanti l'elaborazione di dati da fornire all'interessato in caso di richiesta di accesso ai propri dati;*
- ***diritti di rettifica e di cancellazione:** sono da garantire senza ingiustificato ritardo;*
- ***diritto all'oblio:** nel caso in cui dati personali sono stati trasmessi a terzi, il titolare dovrà informarli della richiesta di rettifica, cancellazione o distruzione dei dati effettuata da parte della persona interessata;*
- ***diritto alla limitazione del trattamento:** in alcuni casi previsti dalla legge, l'interessato può ottenere la limitazione del trattamento dei suoi dati personali; il titolare potrà soltanto conservare i dati, senza possibilità di ulteriori operazioni su di essi;*
- ***diritto alla portabilità dei dati:** su richiesta, il titolare del trattamento deve mettere a disposizione dell'interessato i suoi dati personali su adeguato supporto portatile;*
- ***diritto di opposizione:** l'interessato può opporsi a qualsiasi trattamento che lo riguarda, riservata l'esistenza di un interesse preponderante o di una legge;*
- *diritto a non essere sottoposto a processo decisionale esclusivamente automatizzato;*
- ***diritto alla comunicazione di una violazione dei dati personali:** il titolare del trattamento è tenuto a comunicare all'interessato le violazioni dei dati personali suscettibili di presentare un elevato rischio per i suoi diritti e le sue libertà.»*

(cfr. Messaggio n. 8281 del 17 maggio 2023, pag. 5 di 55)

Revisione totale LPDP

«Per quanto riguarda gli obblighi dei titolari di elaborazioni di dati, è previsto in particolare:

- **principio della responsabilità:** il titolare dell'elaborazione è attivamente responsabile di agire in conformità con il diritto sulla protezione dei dati e, in particolare, di comprovare che l'elaborazione avviene in conformità con quest'ultimo (inversione dell'onere della prova a carico del titolare dell'elaborazione di dati);
- **principio dell'approccio basato sui rischi:** maggiore è il rischio per i diritti e le libertà fondamentali, maggiori sono le responsabilità del titolare del trattamento, che dovrà in particolare mettere in atto misure di sicurezza adeguate ai rischi e meccanismi e sistemi di controllo del rispetto del diritto;
- **principio della protezione dei dati fin dalla progettazione (Privacy by design) e per impostazione predefinita (privacy by default):** le garanzie della protezione dei dati devono essere prese in considerazione sin dalla progettazione dei prodotti e dei servizi;
- **obbligo del registro delle elaborazioni di dati:** ogni grande impresa privata o organo pubblico che elabora dati personali deve tenere un registro delle proprie attività di elaborazione;
- **obbligo della valutazione d'impatto sulla protezione dei dati nei casi in cui un'elaborazione possa presentare un rischio elevato per i diritti e le libertà fondamentali degli interessati;** se sono evidenziati rischi particolari, il titolare del trattamento dovrà consultare l'autorità di controllo indipendente;
- **obbligo di auto-segnalazione:** Il titolare deve notificare all'autorità di controllo indipendente e, in taluni casi, anche alla persona interessata, le violazioni dei dati personali da lui perpetrate, senza ingiustificato ritardo, affinché l'autorità di controllo possa esercitare le sue mansioni legali;
- **obbligo della sicurezza delle elaborazioni:** questo principio implica l'implementazione di misure commisurate ai rischi per i diritti e le libertà fondamentali;
- **obbligo di un'autorità di controllo pienamente autonoma e indipendente:** l'autorità di controllo deve agire in piena autonomia e indipendenza e disporre di tutte le risorse umane, tecniche e finanziarie necessarie per l'effettivo adempimento dei suoi compiti legali.»

(cfr. Messaggio n. 8281 del 17 maggio 2023, pag. 5 di 55)

Revisione totale LPDP – campo di applicazione, art. 3 nLPDP

Art. 3

1Alla legge sottostanno il **Cantone, i Comuni, le altre corporazioni e istituti di diritto pubblico e i loro organi**. A questi sono parificate le persone fisiche e giuridiche di diritto privato, cui siano delegati compiti di diritto pubblico.

2La legge non si applica nella misura in cui uno di questi enti partecipa a una attività economica che non deriva da un potere sovrano (...).

Revisione totale LPDP – campo di applicazione, art. 3 nLPDP

Esempi di corporazioni o istituti di diritto pubblico ex l'art. 3 cpv. 1, prima frase nLPDP



i consorzi di comuni in base alla legge sul consorzio di comuni



i consorzi in base alla legge sui consorzi e per il raggruppamento terreni in base alla legge sul raggruppamento e la permuta dei terreni



i patriziati



le parrocchie



l'Istituto delle assicurazioni sociali (IAS) e organi subordinati quali la Cassa cantonale di compensazione

Revisione totale LPDP – campo di applicazione, art. 3 nLPDP



l'Università della Svizzera italiana (USI)



la Scuola Universitaria professionale della Svizzera italiana (SUPSI)



l'Ente ospedaliero cantonale (EOC)



l'Azienda elettrica ticinese (AET)



l'Azienda cantonale dei rifiuti (ACR)



gli istituti autonomi comunali quali i Trasporti pubblici del Luganese (TPL)



le Aziende industriali del Luganese (AIL)



gli ordini cantonali (dei medici, farmacisti, avvocati, notai, veterinari, ecc.).

Revisione totale LPDP – campo di applicazione, art. 3 nLPDP

Sono invece **delegatari di compiti di diritto pubblico** attraverso delega legislativa, concessione, mandato di prestazione, contratto o altro (art. 3 cpv. 1, seconda frase, nLPDP), in particolare:



I servizi di assistenza e cura a domicilio (SACD)



altri organismi cui sono assegnati compiti pubblici in ambito sanitario



i servizi cui sono affidati compiti pubblici secondo la Legge sull'integrazione sociale e professionale degli invalidi del i servizi preospedalieri e di soccorso



gli organismi che curano programmi occupazionali



le istituzioni o società beneficiarie di un mandato di prestazione quali le cliniche private, le case per anziani, la Società epilettici della Svizzera italiana



aziende delegatarie di trasporti pubblici in base alla legge sui trasporti pubblici le società anonime, le cooperative o le associazioni cui i comuni assegnano compiti e servizi pubblici

Revisione totale LPDP – campo di applicazione, art. 3 nLPDP

- I **delegatari di compiti pubblici** sono sottoposti alla LPDP nella misura in cui la loro attività specifica rientra nell'ambito della delega. Per il resto, sono considerati dei privati e le loro elaborazioni soggiacciono alla legge federale sulla protezione dei dati.
- Quando un organismo secondo il cpv. 1 non agisce nell'ambito del compito pubblico affidatogli, quindi quando non agisce come autorità che per legge detiene un potere pubblico, ma è soggetto alla concorrenza economica, le rispettive elaborazioni di dati sono **sottoposte alle disposizioni della legge federale sulla protezione dei dati applicabili ai privati**.
- In virtù di una convenzione tra **Incaricato federale della protezione dei dati e della trasparenza e Incaricati cantonali**, la sorveglianza sulla corretta applicazione di tali norme federali compete all'Incaricato cantonale della protezione dei dati, che agisce secondo le norme cantonali sulla sorveglianza.

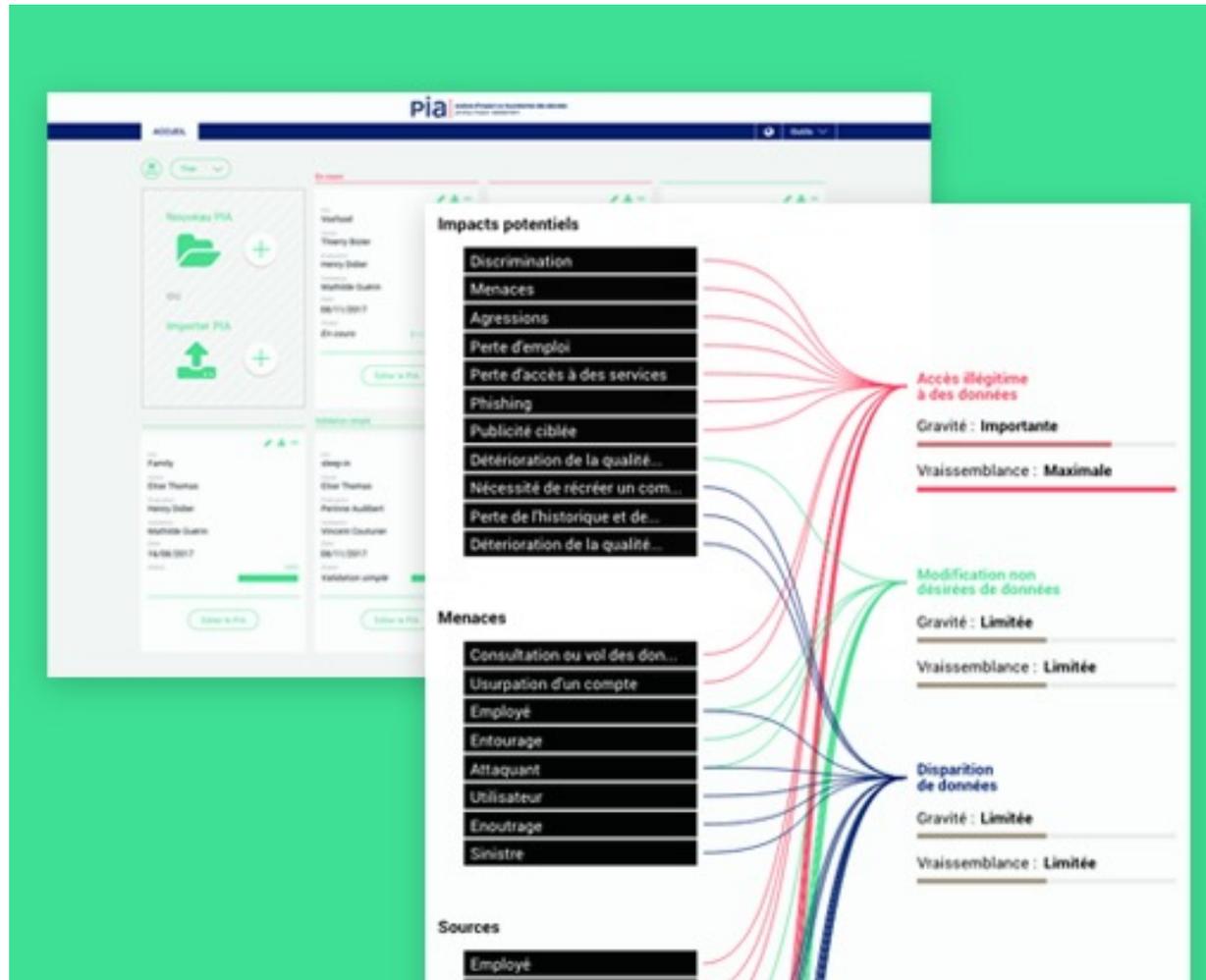
Fonte slide da 11 a 14, Incaricato cantonale

Principi fondamentali delle leggi sulla privacy e strumenti principali;

- ▶ Legalità, equità e trasparenza
- ▶ Limitazione dello scopo
- ▶ Minimizzazione dei dati
- ▶ Precisione
- ▶ Limitazione dell'archiviazione
- ▶ Integrità e riservatezza (sicurezza)
- ▶ Responsabilità
- ▶ TOM (Misure tecniche e organizzative per garantire un livello di sicurezza dei dati adeguato al RISCHIO)
- ▶ Privacy by design
- ▶ Privacy per impostazione predefinita

Principi fondamentali delle leggi sulla privacy e strumenti principali;

- DPIA



Approccio basato sul rischio

- ▶ "Il rischio associato al trattamento deve essere correlato alle possibilità tecniche di ridurlo. Più alto è il rischio, maggiore è la probabilità che si verifichi e più estesa è l'elaborazione dei dati, più alti devono essere i requisiti delle precauzioni tecniche, affinché possano essere considerati adeguati".
- ▶ Identificazione dei rischi associati all'elaborazione.
- ▶ L'analisi del rischio tiene conto della probabilità di accadimento e della gravità delle conseguenze.
- ▶ Classificazione del rischio basso o alto.
- ▶ Trattamento del rischio attraverso misure appropriate.

Very high (4)	4	8	12	16
High (3)	3	6	9	12
Medium (2)	2	4	6	8
Low (1)	1	2	3	4
	Low (1)	Medium (2)	High (3)	Very high (4)

Piano di risposta agli incidenti informatici; cos'è, perché crearlo

- ▶ *"La risposta agli incidenti è un approccio organizzato per affrontare e gestire le conseguenze di una violazione della sicurezza o di un attacco informatico, noto anche come incidente IT, incidente informatico o incidente di sicurezza. L'obiettivo è gestire la situazione in modo da limitare i danni e ridurre i tempi e i costi di recupero".*

Piano di risposta agli incidenti informatici; cos'è, perché crearlo

▶ SANS

- ▶ Preparazione
- ▶ Identificazione
- ▶ Contenimento
- ▶ Sradicamento
- ▶ Recupero
- ▶ Lezioni apprese

▶ NIST

- ▶ Preparazione
- ▶ Rilevamento e analisi
- ▶ Contenimento, sradicamento e recupero
- ▶ Attività post-incidente

DOMANDE?

GRAZIE PER L'ATTENZIONE!

Rocco Talleri

Avvocato – CAS DPO HSG



talleri | **law tech**
services

CP 222
CH - 6925 Collina d'Oro
Tel: +41 (0)91 921 03 37
info@tallerilaw.tech

Riferimenti

- www.cnil.fr
- Prof. D Rosenthal (rosenthal.ch)
- www.nist.gov
- www.sans.org

Copyright Rocco Talleri

Le presenti slides sono a titolo puramente informativo e non costituiscono e non sostituiscono un parere legale