Le norme relative alla protezione dei dati nel mondo

La società in cui viviamo come individui o imprenditori è sempre più digitalizzata. Infatti, l'uso degli strumenti digitali e di Internet si è fortemente democratizzato in molteplici settori, apportando numerosi cambiamenti e facendo nascere nuove modalità di consumo e di interazione.

Oggi numerosi dati vengono digitalizzati, salvati in sistemi informatici e messi online. La protezione dei dati è quindi fondamentale per proteggere le utenti e gli utenti. Per restare competitive, le aziende sono state costrette ad integrare le nuove tecnologie ma anche a mettersi in conformità con i nuovi contesti giuridici. Ad oggi, la questione della protezione dei dati è diventata al contempo cruciale e strategica per garantire la perennità dell'azienda e rafforzare la sua reputazione.

È quindi indispensabile per le aziende comprendere bene i quadri normativi relativi alla protezione dei dati nel mondo per conformarsi ad essi. Questa guida offre alle aziende una panoramica sulle norme relative alla protezione dei dati. Non intende essere esaustiva.

Che cos'è la protezione dei dati e perché regolamentarla ?

Le leggi sulla protezione dei dati proteggono i diritti fondamentali e la personalità delle persone fisiche. Il loro obiettivo principale è proteggere la persona e non il dato stesso. La protezione dei dati fa riferimento alla pratica di proteggere e preservare le informazioni personali e sensibili degli individui o delle organizzazioni contro eventuali accessi, utilizzi, divulgazioni o alterazioni non autorizzati. Essa mira a garantire la riservatezza, l'integrità e la disponibilità dei dati, rispettando al contempo i diritti fondamentali alla privacy e alla protezione dei dati.

Non confondere dati personali e dati sensibili

Secondo la Legge sulla protezione dei dati (LPD), per « dati personali » si intendono tutte le informazioni che riguardano una persona fisica identificata o identificabile.

I dati personali sensibili comprendono i dati sulle opinioni o sulle attività religiose, filosofiche, politiche o sindacali, i dati sulla salute, la sfera intima o l'origine razziale o etnica, i dati genetici, i dati biometrici che identificano una persona fisica in modo univoco, i dati su procedimenti giudiziari o sanzioni penali e amministrative e i dati sulle misure di aiuto sociale.

Questo documento © 2024 dello Stato di Ginevra è concesso in licenza CC BY-SA 4.0
Tutti i contenuti di questo documento possono essere condivisi, copiati, riprodotti, distribuiti, comunicati, riutilizzati e adattati con qualsiasi mezzo e in qualsiasi formato, a condizione che venga citato l'autore (Stato di Ginevra) e che venga utilizzata la stessa licenza per tutti i contenuti correlati (CC - BY - SA 4.0).

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX
h e g Haute école de gestion Genève
UNIVERSITÉ DE GENÈVE

Per saperne di più

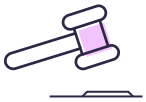
Poste in gioco della protezione dei dati

- **Diritti individuali**
  Garantire alle persone il diritto di controllare, accedere e rettificare i propri dati personali.

- **Minacce crescenti**
  Con lo sviluppo del digitale, i rischi di violazione dei dati sono aumentati, in particolare la distruzione, la perdita, l'alterazione, la divulgazione e l'accesso non autorizzato come, ad esempio, l'hacking.

- **Fiducia dei consumatori**
  Rafforzare la fiducia delle clienti, dei clienti e dei partner verso le aziende, sapendo che i loro dati saranno trattati in modo sicuro.

- **Responsabilità delle aziende**
  Le aziende hanno l'obbligo di adottare misure di sicurezza appropriate e di essere trasparenti sul modo in cui usano i dati.



- **Sanzioni**
  In caso di non conformità, le aziende e/o le persone fisiche possono essere soggette a multe elevate, il che rafforza l'importanza della conformità.

- **Armonizzazione internazionale**
  La normativa aiuta a fissare delle norme comuni per la protezione dei dati nei vari paesi, facilitando gli scambi internazionali di informazioni.

La legge federale sulla protezione dei dati (LPD)

In Svizzera, la legge sulla protezione dei dati è la « Legge federale sulla protezione dei dati » (LPD), in tedesco Datenschutzgesetz (DSG). La prima LPD è del 1992. Con la comparsa di Internet è stata necessaria una revisione completa della LPD per garantire alla popolazione una protezione adeguata dei dati e adattata alle recenti evoluzioni tecnologiche. Una revisione di questa legge era anche indispensabile affinché il diritto svizzero continuasse ad essere compatibile con il diritto europeo, in particolare con il regolamento generale sulla protezione dei dati (GDPR). In questo modo la libera circolazione dei dati con l'Unione Europea è garantita.

La nuova LPD (nLPD) è entrata in vigore il 1° settembre 2023, con effetto immediato, a sostituire integralmente la vecchia legge del 1992. Essa mira a migliorare il trattamento dei dati personali e concede nuovi diritti alle cittadine e ai cittadini svizzeri, pur prevedendo un certo numero di obblighi per le aziende.

Le norme di attuazione della legge, inserite nella nuova « Ordinanza sulla protezione dei dati" (OPDa) e nella nuova "Ordinanza sulle certificazioni in materia di protezione dei dati » (OCPD), sono entrate in vigore contemporaneamente alla nLPD, il 1° settembre 2023.

I 7 principi che guidano la protezione dei dati

- Esattezza
- Sicurezza
- Trasparenza
- Liceità
- Buona fede
- Proporzionalità
- Finalità

Questo documento © 2024 dello Stato di Ginevra è concesso in licenza CC BY-SA 4.0

Un po’ di storia

24 giugno 1976
Adozione della legge sulle informazioni trattate automaticamente al computer (LITAO)

19 giugno 1992
Entrata in vigore della legge federale sulla protezione dei dati (LPD)

25 maggio 2018
Entrata in vigore del regolamento generale sulla protezione dei dati (GDPR)

1 marzo 2019
Revisione parziale della LPD

25 agosto 2023
Entrata in vigore delle norme europee «Digital Services Act» (DSA) e «Digital Market Act» (DMA) per le grandi piattaforme

1 settembre 2023
Entrata in vigore della nuova legge federale sulla protezione dei dati (nLPD)

17 febbraio 2024
Entrata in vigore delle norme europee «Digital Services Act» (DSA) e «Digital Market Act» (DMA) per le piattaforme di piccole dimensioni

Questo documento © 2024 dello Stato di Ginevra è concesso in licenza CC BY-SA 4.0

Le aziende interessate dalla legge sulla protezione dei dati

Tutte le aziende attive in Svizzera o che hanno degli effetti in Svizzera sono interessate e hanno l'obbligo di mettersi in conformità tempestivamente con le nuove disposizioni sulla protezione dei dati.

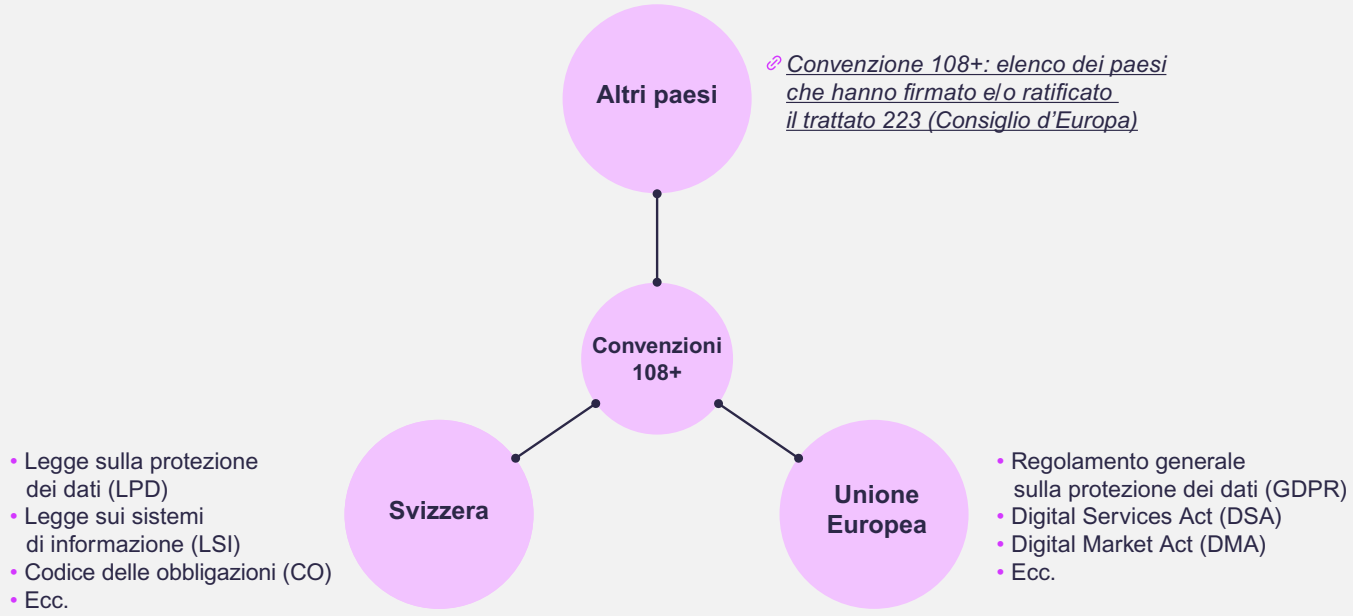
La svizzera e la convenzione 108+

Benché la Svizzera non sia membro dell'Unione Europea, essa ha firmato la Convenzione 108+, impegnandosi ad adottare pratiche simili a quelle degli altri Stati che hanno ratificato questa convenzione in materia di trattamento dei dati personali.

La Convenzione 108+ è un trattato redatto dal Consiglio europeo relativo alla protezione dei dati degli individui nell'ambito del trattamento automatizzato dei loro dati personali. Il suo obiettivo è quello di definire le linee guida della protezione dei dati per garantire il rispetto dei diritti e delle libertà delle persone, in particolare per quanto riguarda la loro privacy quando vengono usate le loro informazioni.

La Convenzione 108 è stata introdotta nel 1981 ed è stato il primo strumento internazionale giuridicamente vincolante. Nel 2018 c'è stato un aggiornamento 2018 chiamato « Convenzione 108+ ». Questo aggiornamento rafforza i diritti degli individui e modernizza i principi di protezione dei dati nell'epoca digitale, in particolare attraverso una maggiore protezione contro i rischi legati ai trattamenti automatizzati.

La Convenzione 108+ è aperta agli Stati che non sono membri del Consiglio europeo. Essa ha quindi effetto anche fuori dall'Europa.



Convenzione 108+: elenco dei paesi che hanno firmato e/o ratificato il trattato 223 (Consiglio d'Europa)

Questo documento © 2024 dello Stato di Ginevra è concesso in licenza CC BY-SA 4.0

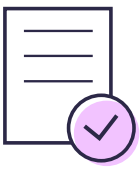
La necessità di rispettare i quadri normativi sulla protezione dei dati personali

Nella maggior parte dei paesi, le norme relative alla protezione dei dati sono state concepite per salvaguardare gli interessi sia degli individui che delle aziende dalle conseguenze dannose di un utilizzo non regolamentato delle informazioni personali. Queste norme non inquadrano solo l'uso dei dati per garantire i diritti delle persone ma fissano in modo più ampio dei principi e delle buone pratiche in materia di raccolta, trattamento e gestione dei dati. Esse assicurano quindi alle aziende e alle persone che devono trattare i dati, il mantenimento della riservatezza e un utilizzo protetto ed etico delle informazioni. In Svizzera, si ricorda che la LPD protegge le persone fisiche ma non le persone giuridiche.

Le infrazioni possono costare caro!
A seconda del paese interessato, della gravità dei fatti e delle norme, le multe possono essere importanti, da poche migliaia di franchi a diversi milioni di franchi.

In Svizzera le sanzioni della LPD riguardano le persone fisiche, con un tetto di CHF 250.000.-. Se non si riescono a trovare gli autori con sforzi proporzionati, la LPD prevede un obbligo di ammenda ulteriore per le aziende a concorrenza di CHF 50.000.- al massimo.

Pene molto più pesanti sono applicate nell'Unione Europea; l'importo delle sanzioni pecuniarie può ammontare fino a 20 milioni di euro o, nel caso di un'azienda, fino al 4% del suo fatturato annuo mondiale.



La messa in conformità con le norme sulla protezione dei dati è essenziale non solo per evitare i rischi giuridici, ma anche per garantire uno sviluppo e una crescita duratura dell'attività. La fiducia digitale è una posta in gioco strategica per le aziende che permette di differenziarsi sul proprio mercato, di conservare e sviluppare la fiducia dei clienti e di garantire la prosperità dell'attività.

«La legge sulla protezione dei dati introduce nuovi obblighi per le aziende, ma si annuncia anche come un vettore di opportunità economiche inedite, propizie all'innovazione e alla crescita settoriale.»

Dessislava Leclère, Professore alla «Haute École de Gestion de Genève»

Questo documento © 2024 dello Stato di Ginevra è concesso in licenza CC BY-SA 4.0

La necessità di rispettare i quadri normativi sulla protezione dei dati personali

Mettersi in conformità rappresenta anche numerose opportunità per le aziende.

- Investire nella protezione dei dati significa investire nella cybersicurezza della propria azienda. Allocando le risorse adeguate alla sicurezza dei dati e dei sistemi di informazioni, le aziende rafforzano la loro resistenza alle minacce e ai rischi legati al digitale.
- Garantendo la riservatezza, l'integrità e la disponibilità dei dati, l'azienda rafforza e sviluppa la sua reputazione e la fiducia presso i clienti, i partner e i team.
- Mettersi in conformità permette a un'azienda di tutelarsi dalle conseguenze provocate da una perdita di fiducia all'interno dell'organizzazione dei clienti o dei partner, come una cattiva pubblicità e una copertura mediatica negativa, la difficoltà di reclutamento e un calo di attrattiva se l'azienda è percepita come negligente in materia di sicurezza, etica e riservatezza.
- Conformandosi ai quadri normativi e anticipando i rischi legati alla protezione dei dati, l'azienda può mantenere l'accesso al mercato e svilupparne di nuovi. Essa evita il rischio di essere esclusa dai contratti pubblici che esigono garanzie di conformità alle norme e pratiche di protezione dei dati.
- Adottare una procedura responsabile e trasparente verso le proprie parti interessate permette all'azienda di promuovere le proprie azioni e i propri valori e di distinguersi dalla concorrenza.
- Adottando misure adeguate di gestione dei rischi digitali, l'azienda evita i rischi finanziari. I rischi possono essere i seguenti : ricevimento di multe, costi legati alla riparazione dei danni subiti dalle parti interessate, costi legati all'adozione di misure correttive dopo un incidente, aumento dei premi assicurativi, calo del valore degli attivi come il database clienti se viene sottratto, ecc.
- Possono verificarsi diversi rischi operativi e tecnici che comportano l'interruzione di tutta o parte dell'attività, impatti sul buon funzionamento operativo e commerciale dell'azienda e un aumento dei rischi di cyber-attacchi se non vengono adottate azioni preventive e normative.
- L'azienda evita un'esposizione a rischi giudiziari e contrattuali se rispetta i quadri normativi vigenti, come i rischi di azioni giudiziarie da parte dei clienti, dei partner o anche dei governi, nonché restrizioni o divieti potenziali di trattare alcuni dati. In questo modo essa si assume anche la responsabilità del buon rispetto del quadro normativo da parte dei suoi subappaltatori. Essa deve quindi far in modo che le leggi vengano applicate correttamente per se stessa e per i suoi subappaltatori.

Preposti alla protezione dei dati

Il Preposto cantonale alla protezione dei dati e alla trasparenza (PPDT) sorveglia l'applicazione della legge cantonale in materia di protezione dei dati e di trasparenza. A Ginevra, al settore pubblico ginevrino si applica la legge sull'informazione del pubblico, l'accesso ai documenti e la protezione dei dati personali (LIPAD).

Il Preposto federale alla protezione dei dati e alla trasparenza (PFPDT) è incaricato di sorvegliare la buona applicazione delle disposizioni federali sulla protezione dei dati. Egli sorveglia, in particolare, il trattamento dei dati eseguito dalle aziende. È anche l'organo di mediazione per l'accesso ai documenti ufficiali.

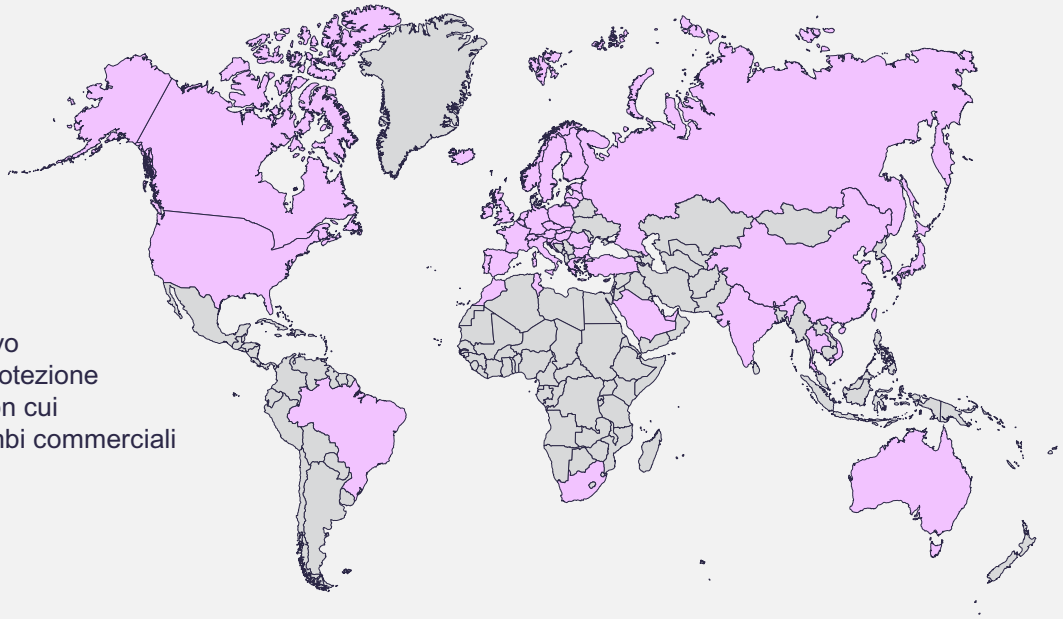
Questo documento © 2024 dello Stato di Ginevra è concesso in licenza CC BY-SA 4.0

I quadri normativi nel mondo

Numerosi dati vengono scambiati ogni giorno online, per questo la necessità di preservare la privacy e di garantire la sicurezza dei dati appare sempre più importante in numerosi paesi.

Secondo la Conferenza delle Nazioni Unite sul commercio e lo sviluppo (CNUCED), alla fine del 2021, 137 paesi su 194 avevano attuato una norma diretta o indiretta per proteggere i dati e la privacy.

Elenco non esaustivo delle norme sulla protezione dei dati dei paesi con cui la Svizzera ha scambi commerciali



Svizzera	Loi sur la protection des données (LPD) / Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) / Nuova legge sulla protezione dei dati (LPD)	2023
Unione Europea	Regolamento generale sulla protezione dei dati (GDPR)	2018
Regno Unito	UK General Data Protection Regulation	2021
Norvegia	Personvernforordningen GDPR	2021
Islanda	Almenna persónuverndarreglugerði	2018
Turchia	Kişisel verilerin korunmasi kanunu	2016
Stati Uniti	Lois spécifiques par État	2020
Canada	Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)	2020
Brasile	Lei Geral de Proteção de Dados Pessoais	2020
Tunisia	Loi sur la protection des données à caractère personnel	2004
Marocco	Loi relative à la protection des données des personnes physiques à l'égard des traitements des données à caractère personnel	2009
Sudafrica	The Protection of Personal Information Act (POPIA)	2020
Emirati Arabi Uniti	القانون الاتحادي بشأن حماية البيانات الشخصية	2021
Russia	О персональных данных	2006
India	Information Technology Act	2020
Cina	Personal information protection law (PIPL)	2021
Hong-Kong	Personal Data (Privacy) Ordinance	1996
Giappone	個人情報の保護に関する法律	2017
Corea del Sud	개인정보 보호법	2011
Taiwan	Personal Data Protection Act	2015
Singapore	Personal Data Protection Act	2012
Tailandia	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล	2019
Vietnam	Nghị định bảo vệ dữ liệu cá nhân (Nghị định BVDLCN)	2023
Australia	Privacy Act	1988

Questo documento © 2024 dello Stato di Ginevra è concesso in licenza CC BY-SA 4.0

Obblighi relativi alle norme sulla protezione dei dati

Stati in cui è garantito un livello di protezione adeguato dei dati	**Valutazione del livello di protezione adeguato comprendente i trasferimenti dei dati.** *Data Protection Ordinance (OPDo)*
Obbligo di informazione	Tutte le aziende hanno l'obbligo di comunicare in modo chiaro e trasparente alle persone e/o alle entità interessate le finalità, le fonti e i metodi di trattamento dei dati personali.
Registro delle attività	Le aziende sono tenute a mantenere aggiornato un registro delle loro attività che recensisca tutte le operazioni di trattamento dei dati personali.
Analisi di impatto	A seconda della categoria di dati trattati dalle aziende, queste devono eseguire un'analisi di impatto sui rischi del trattamento dei dati personali per garantirne la protezione.
Consenso in caso di trattamento dei dati sensibili	A seconda del tipo di trattamento e dei dati trattati, le aziende devono ottenere il consenso esplicito e informato delle persone di cui trattano i dati.
Notifica di casi di violazione dei dati	Le aziende sono tenute ad informare le autorità e, eventualmente, le persone interessate nel caso si verifichi una faglia nella sicurezza che comporti l'accesso, la divulgazione o la perdita di dati personali.
Privacy by design/di default	Le aziende devono integrare la protezione dei dati sin dalla progettazione di un prodotto o di un servizio ("privacy by design"). Inoltre, le configurazioni predefinite dei servizi o dei software devono garantire il livello più alto di riservatezza e di sicurezza senza l'intervento dell'utente (privacy di default).
Presenza di un delegato alla protezione dei dati	Le aziende sono tenute a nominare una persona responsabile della protezione dei dati personali (delegato alla protezione dei dati) che vegli sul rispetto delle norme vigenti.
Sanzioni	Le aziende sono passibili di sanzioni in caso di violazione delle leggi sulla protezione dei dati.
Diritto alla trasparenza per le persone	Le aziende devono informare gli individui sul modo in cui i loro dati personali sono raccolti, usati e condivisi.
Diritto di accesso	Le aziende hanno l'obbligo di fornire alle persone che glielo chiedono una copia dei dati personali che esse detengono.
Diritto di rettifica	Le aziende sono tenute a correggere o aggiornare le informazioni personali inesatte o incomplete che detengono a richiesta di un individuo.
Diritto di cancellazione	Le aziende hanno l'obbligo di cancellare i dati personali degli individui che ne fanno richiesta.
Diritto di limitazione del trattamento	In alcune circostanze specifiche, le aziende devono limitare temporaneamente il trattamento dei dati di una persona, se questa glielo chiede.
Diritto di portabilità	Le aziende hanno l'obbligo di trasmettere i dati personali agli individui che ne fanno richiesta in un formato di uso comune e di trasferirli a un'altra azienda, se richiesto.
Diritto di opposizione	Le aziende devono permettere agli individui di opporsi al trattamento dei loro dati personali per motivi legittimi.
Diritto di non essere oggetto di una decisione interamente automatizzata	Gli individui possono chiedere alle aziende che il trattamento automatizzato dei loro dati che porti a una decisione prevista sia rivisto da una persona.

Questo documento © 2024 dello Stato di Ginevra è concesso in licenza CC BY-SA 4.0

Comparative table

	Svizzera	Unione Europea	Regno Unito	Norvegia	Islanda	Turchia	Stati Uniti	Canada	Brasile	Tunisia	Marocco	Sudafrica	Emirati arabi uniti	Russia	India	Cina	Hong Kong	Giappone	Corea del Sud	Taiwan	Singapore	Tailandia	Vietnam	Australia
Stati in cui è garantito un livello di protezione adeguato dei dati	●	●	●	●	●			●																
Obbligo di informazione	●	●	●	●	●	●	●	●	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	●
Registro delle attività	●	●	●	●	●	●	○	●	●	●	●	●							○			○	●	
Analisi di impatto	●	●	●	●	●	○	○	●	●			●	○	○	○	●							●	
Consenso in caso di trattamento dei dati sensibili	●	●	●	●	●	●	○	●	●	●	●	●	●	●		●	○	●	●	●	●	●	●	●
Notifica di casi di violazioni dei dati	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●			●	●	●	●	●	●
Privacy by design/di default	●	●	●	●	●	○	○	●	○														●	
Presenza di un delegato alla protezione dei dati	○	●	●	●	●	○	○	●	●	○	○	●	○	○	○	●			●		●	○	○	
Sanzioni	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Diritto alla trasparenza per le persone	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●	●	●	●
Diritto di accesso	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●
Diritto di rettifica	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Diritto di cancellazione	●	●	●	●	●	●	○	●	●	●	○	●	●	●	○	○	○	●	●	○	○	●	●	○
Diritto di limitazione del trattamento	●	●	●	●	●	●	○	●	●	●		●	●			●		○	●			●	●	
Diritto di portabilità	●	●	●	●	●		○		●	●			●			●			●			●	●	
Diritto di opposizione	●	●	●	●	●	●	○	●	●	●	●	●	●		●	●	○	○	●		●	●	●	
Diritto di non essere oggetto di una decisione interamente automatizzata	●	●	●	●	●	○	○	●	●	●		○	●	○		○			●					

● = *Sì*
○ = *Sì in certi casi, stati o province.*

Fare sempre riferimento alle norme vigenti. Queste informazioni sono fornite a titolo indicativo.
È sempre bene verificare le informazioni leggendo le norme vigenti nel paese interessato.

Questo documento © 2024 dello Stato di Ginevra è concesso in licenza CC BY-SA 4.0

Tappe per una gestione ottimale dei dati e della conformità normativa

Identificare i mercati in cui l'azienda è attiva. Occorre innanzitutto elencare i paesi, le regioni o gli stati in cui l'azienda è attiva. Poi occorre identificare i tipi di attività commerciali o gestionali che l'azienda esercita in queste regioni e stabilire se sono soggette alle norme vigenti.

Leggere e comprendere le norme vigenti nei paesi in cui l'azienda è attiva. I quadri normativi variano a seconda delle regioni e del tipo di attività delle aziende. È indispensabile informarsi sulle norme vigenti nei paesi in cui l'azienda è attiva per essere in regola con le leggi in vigore.

Raccogliere unicamente i dati necessari. Occorre assicurarsi che il trattamento dei dati sia lecito e ridurre allo stretto necessario la raccolta di dati limitandosi alla finalità del trattamento stabilito dall'azienda e annunciato in occasione della raccolta dei dati. È anche necessario precisare per quanto tempo queste informazioni dovranno essere conservate.

Catalogare e mappare i dati detenuti dall'azienda. Questa operazione permetterà di identificare le eventuali informazioni che l'azienda non dovrebbe possedere per mettersi in conformità e applicare il trattamento richiesto di questi dati.

Gestire il ciclo di vita dei dati. È importante stabilire per quanto tempo saranno necessari i dati raccolti e fissare una data di cancellazione dei dati. Quando i dati non sono più necessari per le finalità del trattamento, devono essere distrutti o anonimizzati.

Sviluppare e applicare una politica di trasparenza nel trattamento dei dati. Proprio come durante la raccolta dei dati, è indispensabile essere trasparenti per quanto riguarda i dati detenuti, l'obiettivo del loro trattamento e l'utilizzo previsto dall'azienda o dai suoi partner.

Proteggere i dati. È importante adottare tutte le misure necessarie per proteggere i dati detenuti e gestiti dall'azienda. Ciò riguarda in particolare i provvedimenti tecnici e la formazione di chiunque abbia accesso ai dati.

Per maggiori informazioni, consultare la guida ai cyber-rischi.

Ginevra, cantone pioniere in materia di diritto all'integrità digitale
Il 18 giugno 2023, gli abitanti di Ginevra hanno accettato al 94,21% la modifica della costituzione della Repubblica e cantone di Ginevra per introdurre un diritto fondamentale volto a tutelare l'integrità digitale delle cittadine e dei cittadini, principalmente nell'ambito delle loro relazioni con le pubbliche amministrazioni.

Questo documento © 2024 dello Stato di Ginevra è concesso in licenza CC BY-SA 4.0