Aiuto all'implementazione da FIDUCIAIRI|SUISSE

Novembre 2022

Utilizzando le domande e le istruzioni che seguono, potete implementare i nuovi requisiti della revisione della legge sulla protezione dei dati nella vostra società fiduciaria. A seconda di come rispondete alle singole domande per la vostra azienda, non dovete fare nulla oppure potete seguire le istruzioni sui singoli argomenti e adattare i vostri processi, le linee guida interne, i contratti, ecc. Troverete altri modelli nell'area riservata ai soci del sito web di FIDUCIARI|SUISSE.

Questa guida non pretende di essere completa e non costituisce una consulenza legale. Vi invitiamo a consultare anche la nuova legge e la relativa ordinanza e a rivolgervi a specialisti della protezione dei dati in caso di ulteriori dubbi. Ulteriori informazioni sulla legge sulla protezione dei dati sono disponibili sul sito web dell'Ufficio federale di giustizia: https://www.bj.admin.ch/bj/it/home/staat/gesetzgebung/datenschutzstaerkung.html

Domanda	Risposta	Risposta
Avete una **dichiarazione di protezione dei dati** aggiornata per il vostro sito web, i suoi contratti, la vostra conferma d'ordine, ecc.	☐ sì non dovete fare nulla	☐ no ➔ vedi par. 1
Avete delle **linee guida** interne per il trattamento dei dati (dati dei clienti, dati salariali dei vostri clienti, ecc.)?	☐ sì non dovete fare nulla	☐ no ➔ vedi par. 2
Avete un **elenco** aggiornato di tutti i dati elaborati nella vostra azienda?	☐ sì non dovete fare nulla	☐ no ➔ vedi par. 3
Avete una procedura per rispondere tempestivamente alle **richieste di informazioni** (ad esempio, richieste di informazioni o di cancellazione di dati)?	☐ sì non dovete fare nulla	☐ no ➔ vedi par. 4
Disponete di un processo per la segnalazione tempestiva di una **violazioni** della protezione dei dati (chi segnala cosa a chi e con quale tempistica)?	☐ sì non dovete fare nulla	☐ no ➔ vedi par. 5
Avete controllato i **subappaltatori** o i loro contratti per assicurarvi che la sicurezza dei dati personali sia garantita, che trattino i dati personali solo nel modo in cui li trattano loro stessi e che abbiate ottenuto il vostro consenso prima di ingaggiare un subappaltatore? e avete aggiunto clausole appropriate?	☐ sì non dovete fare nulla	☐ no ➔ vedi par. 6
Avete un processo per la **cancellazione** o rendere anonimi tutti i dati personali di una persona coinvolta?	☐ sì non dovete fare nulla	☐ no ➔ vedi par. 7
I vostri dati sono conservati **esclusivamente in Svizzera**? In caso contrario, avete verificato se questi Paesi sono presenti nell'elenco del Consiglio federale e avete adottato ulteriori misure?	☐ sì non dovete fare nulla	☐ no ➔ vedi par. 8
Avete fatto **controllare** i vostri processi e la vostra **infrastruttura IT** per verificare se soddisfano uno standard di sicurezza adeguato attraverso misure tecniche e organizzative aggiornate (ad es. direttive sulle password, il vostro partner IT ha installato gli ultimi aggiornamenti, firmware, ecc.)?	☐ sì non dovete fare nulla	☐ no ➔ vedi par. 9
Trasmettete **dati personali particolarmente sensibili**?	☐ no non dovete fare nulla	☐ sì ➔ vedi par. 10
Offrite **l'output dei dati** in un formato elettronico comune?	☐ sì non dovete fare nulla	☐ no ➔ vedi par. 11
Conoscete il termine **valutazione d'impatto sulla protezione dei dati** ed eseguite tali valutazioni quando necessario?	☐ sì non dovete fare nulla	☐ no ➔ vedi par. 12

1. Dichiarazione di protezione dei dati personali

Avete bisogno di una dichiarazione di protezione dei dati sul vostro sito web?
Avete bisogno di una dichiarazione sulla privacy nei contratti con i vostri clienti?

Poiché in qualità di fiduciario vi procurate inevitabilmente dati personali, dovete informare per quale scopo trattate i dati personali, a chi li comunicate (non singoli nomi, ma categorie di destinatari, ad esempio "società del gruppo", "partner", "fornitori di servizi IT", "autorità", ecc.), se ed eventualmente quali dati vengono ottenuti da terzi (cioè non dall'interessato stesso) e se i dati vengono trasferiti all'estero. La formulazione di una dichiarazione di protezione dei dati- o di più informative - è quindi un compito importante nella preparazione alla nuova legge.

Nell'adempimento dell'obbligo di informazione, molto spesso ci si chiede se sia sufficiente fare riferimento a una dichiarazione sulla protezione dei dati su Internet da un documento stampato, ad esempio le CGC o una comunicazione scritta. Riteniamo che una pubblicazione su Internet sia sufficiente se si rimanda almeno al sito web. [1]

L'interessato (ad esempio il vostro cliente) può anche influenzare il trattamento dei dati attraverso il consenso, legittimando un trattamento che altrimenti sarebbe inammissibile. Tuttavia, ciò è necessario solo in casi eccezionali, poiché la FADP e la revDSG non richiedono una base giuridica speciale. È sufficiente per rispettare i principi di trattamento. Il consenso è quindi necessario solo se il trattamento supera l'ambito consentito, ad esempio se i dati personali particolarmente sensibili vengono trasmessi a terzi.

Potete inviare al vostro cliente una dichiarazione di protezione dei dati al momento dell'accettazione del mandato o rimandarlo alla dichiarazione di protezione dei sul vostro sito web. Potete anche utilizzare diverse informative sulla privacy, ad esempio una versione per i soli visitatori del vostro sito web.

Avete bisogno di una dichiarazione di protezione dei dati sul vostro sito web? Anche se non raccogliete dati sul vostro sito web e i visitatori non possono inserire alcun dato, vi consigliamo di pubblicare una dichiarazione sulla privacy sul vostro sito web. Se non vengono raccolti dati, questo potrebbe essere menzionato nella dichiarazione di protezione dei dati. Tuttavia, i siti web hanno spesso almeno un modulo di contatto. Lo scopo è quello di stabilire un contatto. A questo scopo, ad esempio, viene integrato un servizio di moduli dagli Stati Uniti. Quando qualcuno compila il modulo, le informazioni vengono memorizzate da questo servizio di formulari e voi ricevete le informazioni anche via e-mail. Le informazioni comprendono nomi e indirizzi e-mail e messaggi. Inoltre, ci sono data e ora e indirizzi IP come metadati. In questo modo si ottiene una raccolta di dati e la si elabora. Dovete informare i visitatori del sito web, preferibilmente in una dichiarazione sulla privacy.

La dichiarazione di protezione dei dati deve contenere in particolare le seguenti informazioni:

- Chi è il responsabile del trattamento dei dati e come si può contattare?[2]
- Per quale/i scopo/i vengono trattati i dati personali?
- Chi sono i destinatari dei dati personali trattati e in quali Paesi/regioni si trovano?
- Come viene garantita l'esportazione dei dati?
- Quali diritti hanno gli interessati in relazione alla protezione dei dati?

[1] Si veda l'articolo professionale del Dr. David Vasella „Das neue Datenschutzgesetz und seine Umsetzung", publicato su TREX, numero 5/21
[2] È sufficiente un indirizzo e-mail generico: protezione dei dati@impresa.ch

2. linee guida per il trattamento dei dati

Si consiglia di redigere delle linee guida per il trattamento dei dati all'interno dell'azienda. Dovrebbero essere inclusi i seguenti punti:

- Chi ha accesso* a quali dati
- Chi può trattare i dati
- Dove devono essere conservati i dati
- Come/quando i dati vengono cancellati
- quali dati possono essere inviati solo in forma criptata
- Quali regole si applicano al trattamento dei dati (uso di password, clean desk, ecc.) Nell'area riservata ai membri di FIDUCIARI|SUISSE troverete ulteriori aiuti su questo argomento.
- Regole speciali

La documentazione dei processi è utile per le indagini ufficiali o per eventuali procedimenti legali.

*I diritti di accesso devono essere costantemente aggiornati in tutte le soluzioni software e le strutture di cartelle. Soprattutto in caso di cambiamenti del personale, l'aggiornamento deve essere previsto nel corrispondente processo HR.

3. Registro di tutti i trattamenti di dati

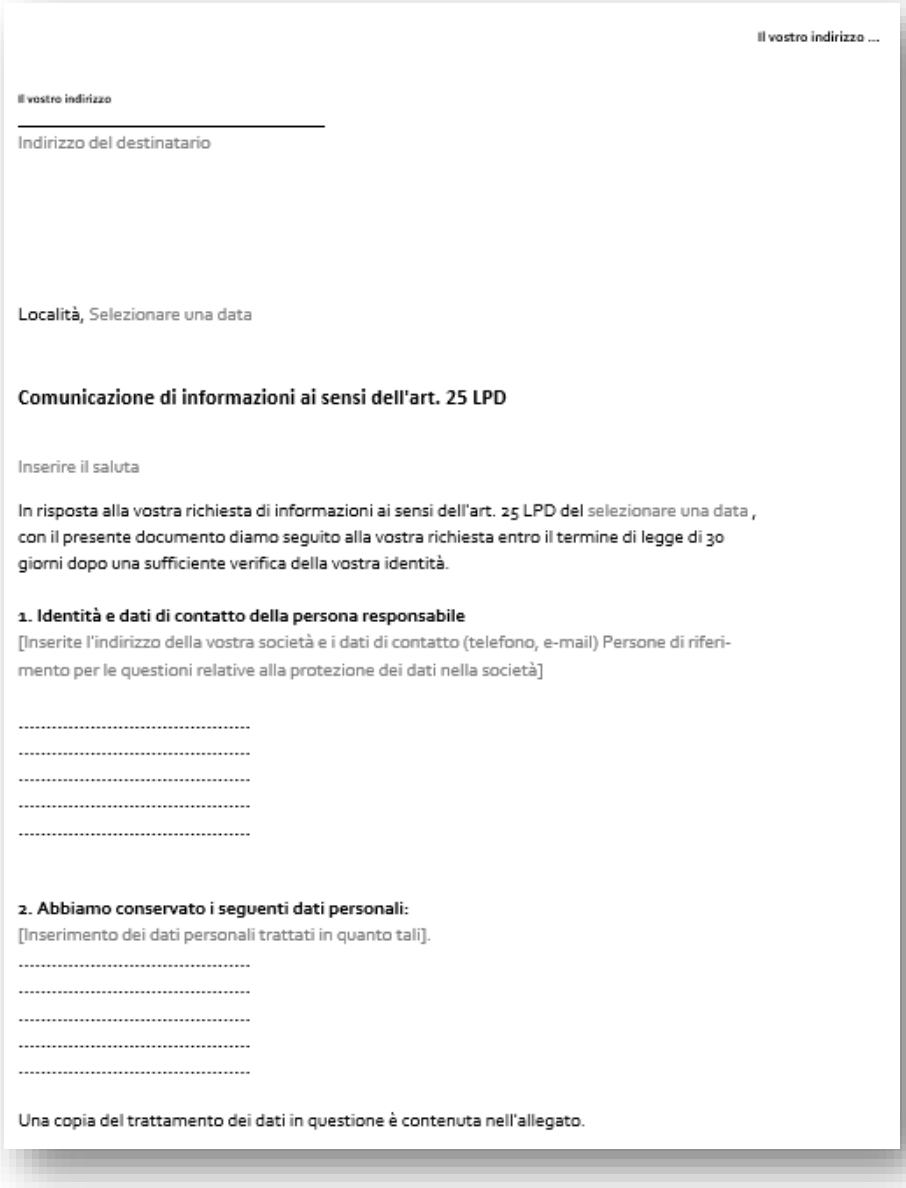
Le aziende con meno di 250 dipendenti non sono tenute a tenere un registro, a meno che non vi sia un rischio elevato per gli interessati. Sebbene le società fiduciarie non presentino di solito un rischio elevato per le persone interessate (clienti e dipendenti), raccomandiamo di tenere un registro in ogni caso, poiché questa panoramica aiuta a soddisfare vari altri requisiti della revDSG. È sufficiente un semplice elenco in Excel o Word. Un modello di esempio è disponibile sul sito web di FIDUCIARI|SUISSE.

Esempio:

Attività di trattamento									Foglio 1
Nr.	responsabilità condivise	Scopo	Categorie di persone colpite	Categorie Dati personali	Destinatario	Trasmissione a cui Paesi terzi	Scadenze di cancellazione	Misure tecniche ed organizzative	Data dell'ultima modifica
01	-	Contabilità paghe	Collaboratori	Dati anagrafici e dati contrattuali, dati di conto corrente bancario, Dati di assicurazioni sociali, dati di busta paga o dati salariali	Dipartimento risorse umane, ufficio paghe esterno, Assicurazione sociale	no	dopo la scadenza dei termini legali o della prescrizione di eventuali richieste legali (da specificare esattamente)	Aumento del livello di protezione - misure in base al concetto di sicurezza: ad es. Reparto personale separato area di accesso separata; Controllo degli accessi Dati	1.4.2022
02	-	Registrazione dell'orario di lavoro	Collaboratori	Dati anagrafici e contrattuali, orari di lavoro, malattie, ferie, altro assenze	Risorse umane	no	dopo la scadenza dei termini legali o della prescrizione di eventuali richieste legali (da specificare esattamente)	Livello di protezione aumentato - misure secondo concetto di sicurezza: Controllo dell'accesso ai dati	3.5.2022
03	-	Gestione dei viaggi	Collaboratori	Dati anagrafici, dati di prenotazione, dati di legittimazione (numero di carta di credito)	FFS, Swiss o altre compagnie aeree, Agenzia di viaggi	si, per viaggi all'estero con compagnie aeree straniere o per i visti	dopo la scadenza degli obblighi di conservazione previsti dalla legge commerciale o fiscale (da specificare esattamente)	Livello di protezione normale - Nessuna misura speciale necessaria	1.4.2022
04	-	Assistenza clienti	Clienti attivi ed ex clienti	Dati anagrafici, contrattuali e di dati sulle prestazioni, dati di fatturazione, corrispondenza, ecc.	Contabilità finanziaria, vendite	no	dopo la scadenza degli obblighi di conservazione previsti dalla legge commerciale o fiscale (da specificare esattamente)	vedere sopra	4.5.2022
05		Approvvigionamento	Fornitori (se persona fisica)	dettagli di contatto operativi, informazioni su conoscenze e competenze	Dipartimento acquisti interno	no	dopo la scadenza degli obblighi di conservazione previsti dalla legge commerciale o fiscale (da specificare esattamente)	vedere sopra	4.5.2022

4. Richiesta di informazioni

Gli interessati (clienti, visitatori del sito web, ecc.) hanno numerosi diritti in relazione al trattamento dei loro dati. Possono presentare una richiesta di informazioni o di cancellazione. Tali richieste devono essere soddisfatte entro un breve periodo di tempo (di solito entro 30 giorni). Stabilite chi è responsabile di rispondere alle richieste. L'elenco di tutti i trattamenti dei dati (sezione 3) aiuta a raccogliere le informazioni pertinenti.
Anche se non si può presumere che molti clienti delle società fiduciarie presentino una richiesta di informazioni, si raccomanda comunque di preparare un processo corrispondente, compreso un modello.
Un modello di lettera di risposta è disponibile nell'area riservata ai soci del sito web di FIDUCIARI|SUISSE.



Il vostro indirizzo ...

Il vostro indirizzo

Indirizzo del destinatario

Località, Selezionare una data

Comunicazione di informazioni ai sensi dell'art. 25 LPD

Inserire il saluta

In risposta alla vostra richiesta di informazioni ai sensi dell'art. 25 LPD del selezionare una data , con il presente documento diamo seguito alla vostra richiesta entro il termine di legge di 30 giorni dopo una sufficiente verifica della vostra identità.

1. Identità e dati di contatto della persona responsabile
[Inserite l'indirizzo della vostra società e i dati di contatto (telefono, e-mail) Persone di riferimento per le questioni relative alla protezione dei dati nella società]

.....
.....
.....
.....
.....

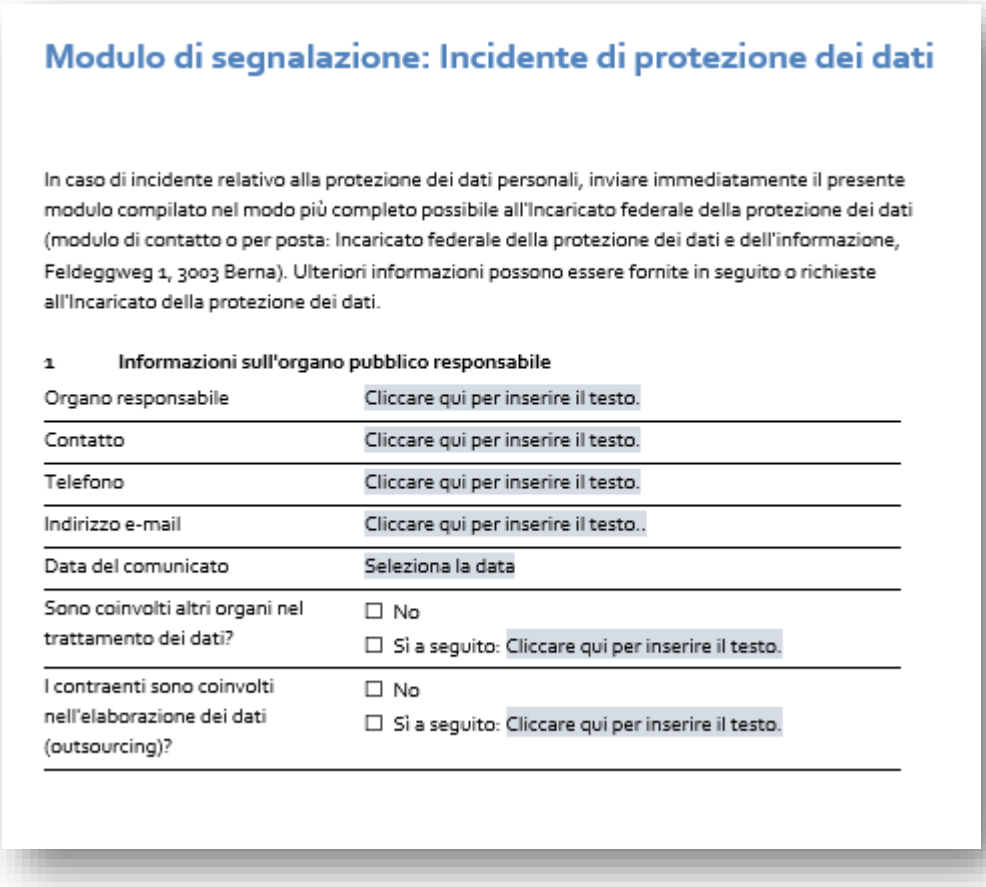
2. Abbiamo conservato i seguenti dati personali:
[Inserimento dei dati personali trattati in quanto tali].
.....
.....
.....
.....
.....

Una copia del trattamento dei dati in questione è contenuta nell'allegato.

5. Processo di notifica della violazione dei dati

Una violazione della protezione dei dati si verifica quando i dati personali vengono persi, cancellati o alterati involontariamente o illegalmente o divulgati o resi accessibili a persone non autorizzate. Tali notifiche di violazioni che comportano un rischio elevato di compromissione della personalità o dei diritti fondamentali degli interessati devono essere segnalate all'Incaricato federale della protezione dei dati IFPDT il più presto possibile (nell'UE entro 72 ore). Se il rischio è basso, la segnalazione può essere fatta volontariamente. Al fine di tutelare l'interessato, quest'ultimo deve essere informato anche in caso di rischio elevato di compromissione. Gli incaricati del trattamento (quindi eventualmente anche i fornitori di servizi esterni) devono segnalare tempestivamente al titolare del trattamento tutte le violazioni della sicurezza dei dati.
Sono necessarie misure organizzative e tecniche per poter rilevare immediatamente una violazione dei dati. Un registro di tutte le attività di trattamento dei dati aiuta a individuare eventuali violazioni della protezione dei dati (sezione 3).

Un modello di notifica all'IFPDT è disponibile sul sito web di FIDUCIARI|SUISSE.



Modulo di segnalazione: Incidente di protezione dei dati

In caso di incidente relativo alla protezione dei dati personali, inviare immediatamente il presente modulo compilato nel modo più completo possibile all'Incaricato federale della protezione dei dati (modulo di contatto o per posta: Incaricato federale della protezione dei dati e dell'informazione, Feldeggweg 1, 3003 Berna). Ulteriori informazioni possono essere fornite in seguito o richieste all'Incaricato della protezione dei dati.

1 Informazioni sull'organo pubblico responsabile

Organo responsabile	Cliccare qui per inserire il testo.
Contatto	Cliccare qui per inserire il testo.
Telefono	Cliccare qui per inserire il testo.
Indirizzo e-mail	Cliccare qui per inserire il testo..
Data del comunicato	Seleziona la data
Sono coinvolti altri organi nel trattamento dei dati?	☐ No ☐ Sì a seguito: Cliccare qui per inserire il testo.
I contraenti sono coinvolti nell'elaborazione dei dati (outsourcing)?	☐ No ☐ Sì a seguito: Cliccare qui per inserire il testo.

6. Esaminare i contratti con i subappaltatori/fornitori di servizi.

I servizi di terze parti sono utilizzati per molte funzioni, ad esempio per l'invio di e-mail e newsletter, per il software di contabilità nel cloud, per i fornitori di software-as-a-service o per le videoconferenze. Probabilmente anche voi lavorate con fornitori di servizi.
L'esternalizzazione dell'elaborazione dei dati a subappaltatori è possibile se sono soddisfatti i seguenti requisiti:

- Non vengono violati gli obblighi di riservatezza
- L'incaricato dell'elaborazione degli ordini può trattare i dati solo nel modo in cui il cliente stesso è autorizzato a farlo. Non sono consentiti cambi di destinazione d'uso
- L'incaricato del trattamento deve essere in grado di garantire la sicurezza dei dati.
- Il trattamento in subappalto può avvenire solo previa autorizzazione.

Verificare i contratti con i subappaltatori per assicurarsi che la sicurezza dei dati sia garantita e, se necessario, aggiungere clausole appropriate (in particolare per quanto riguarda la segnalazione di eventuali violazioni della protezione dei dati). Per quanto riguarda le clausole, vedere anche il punto 8.
Raccomandiamo inoltre di includere un obbligo di notifica delle violazioni dei dati e un obbligo di autorizzazione per il subappalto.

7. Quando devono essere cancellati i dati?

L'azienda deve cancellare i dati personali che non sono più necessari e il cui trattamento non può essere giustificato. I dati sono correttamente cancellati se non possono essere recuperati senza uno sforzo sproporzionato. Utilizzate l'elenco delle vostre attività di trattamento dei dati (sezione 3) per verificare se avete pianificato un processo di cancellazione per tutte le attività di trattamento dei dati.

8. Trasferimento dei dati all'estero

La maggior parte dei fornitori di cloud e di software-as-a-service (software di contabilità, newsletter via e-mail, CRM, ecc.) dispone di server al di fuori della Svizzera. I dati personali possono essere divulgati all'estero se la legislazione dello Stato interessato (o dell'organismo internazionale) garantisce una protezione adeguata. L'IFPDT, o in futuro il Consiglio federale in base alla revisione della legge sulla protezione dei dati, gestisce un elenco di "Paesi terzi sicuri"; si veda l'elenco dei Paesi qui. Nel caso di "Paesi terzi non sicuri", ad esempio gli Stati Uniti, sono necessarie clausole contrattuali aggiuntive e ulteriori misure di sicurezza.

In caso di esportazione di dati negli Stati Uniti (ovvero anche di memorizzazione di dati personali su server negli Stati Uniti), ad esempio utilizzando un servizio Internet negli Stati Uniti, è possibile garantire un'adeguata protezione dei dati con le cosiddette clausole contrattuali standard (SCC) e con altre misure di sicurezza (anonimizzazione, crittografia, ecc.). Se esportate dati negli Stati Uniti o utilizzate fornitori di servizi statunitensi, dovete verificare se tali clausole contrattuali standard sono menzionate o incluse. Spesso fanno parte delle CGC o del GPC (contratto di elaborazione degli ordini). In caso contrario, dovete assicurarvi che tali clausole siano incluse. Dovete inoltre valutare l'utilizzo di ulteriori misure di sicurezza nell'ambito di una valutazione del rischio e, se necessario, di una valutazione dell'impatto sulla protezione dei dati (DIA). La valutazione dell'ammissibilità dell'esportazione di dati negli Stati Uniti può cambiare continuamente. Si prega di consultare regolarmente la pagina corrispondente dell'IFPDT.

9. Infrastruttura IT

A seconda del rischio dei dati, devono essere adottate misure tecniche e organizzative adeguate. I dati personali del dipartimento HR sono particolarmente sensibili e devono essere trattati con cura. Anche i fiduciari conservano dati sensibili dei clienti e devono quindi dare la massima priorità alla sicurezza dei dati.

Per garantire la sicurezza dei dati, si consiglia di far controllare l'infrastruttura informatica da uno specialista esterno. Questo specialista verifica se

- siano state adottate misure organizzative (ad es. direttive interne, direttive sulle password, gestori di password, formazione/sensibilizzazione dei dipendenti, ecc.)
- se tutti i software sono aggiornati con tutti gli update rilevanti per la sicurezza
- se tutti i dispositivi sono protetti con moderni scanner antivirus
- se è in uso un firmware aggiornato
- se il firewall è configurato correttamente
- se il back-up dei dati viene eseguito correttamente.

Anche se avete un partner IT esterno, non potete essere sicuri che tutti i punti sopra menzionati siano soddisfatti. Inoltre, la "frode" è uno degli incidenti informatici più frequenti e il punto debole è l'essere umano (password). È qui che entrano in gioco le misure organizzative piuttosto che quelle tecniche.
FIDUCIARI|SUISSE collabora con partner che effettuano controlli di sicurezza per i nostri membri. Potete trovarli all'indirizzo: https://www.treuhandsuisse.ch/it/informazioni-sulla-cibersicurezza.

10. dati personali che richiedono una protezione speciale

Anche i dati personali che richiedono una protezione speciale devono essere protetti in modo particolare e trasmessi solo in forma criptata. Si tratta, tra l'altro, di

- dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche di una persona
- l'appartenenza a un sindacato
- dati genetici, dati biometrici trattati al solo fine di identificare in modo univoco una persona fisica
- dati sulla salute
- dati relativi alla vita sessuale o all'orientamento sessuale di una persona.
- dati relativi a procedimenti e sanzioni amministrative o penali
- dati relativi a misure di assistenza sociale

Le società fiduciarie hanno maggiori probabilità di accedere, conservare o inviare dati personali appartenenti alle ultime due categorie.
I dati relativi alle retribuzioni non rientrano tra i dati personali che richiedono una protezione particolare. Si consiglia comunque di confermare che tali dati possono essere inviati in forma non criptata.

11. Portabilità dei dati

Con il diritto alla portabilità dei dati, l'interessato ha la possibilità di chiedere che i suoi dati personali, che ha comunicato a un responsabile del trattamento privato, gli vengano trasferiti in un formato elettronico comune o a un terzo. Il prerequisito è che i dati siano trattati automaticamente e con il consenso dell'interessato o in diretta connessione con un contratto.
Questo diritto, che probabilmente è più vicino alla legge antitrust che a quella sulla protezione dei dati, ha lo scopo di facilitare il cambio di fornitore nell'interesse della concorrenza. Resta da vedere quale significato avrà nella pratica.

In qualità di membri di FIDUCIARI|SUISSE, siete anche obbligati dal Codice di Condotta Professionale a consegnare i dati dei clienti.

12. Valutazione dell'impatto sulla protezione dei dati

Le aziende devono valutare in ogni caso i rischi derivanti dal trattamento dei dati personali. Spesso è sufficiente una valutazione intuitiva del rischio. Tuttavia, alcune operazioni di trattamento sono più sensibili. In questi casi, sono necessarie considerazioni più approfondite. Se un trattamento può comportare rischi elevati, la nuova legge sulla protezione dei dati impone al responsabile del trattamento di valutare e documentare i rischi nell'ambito di una valutazione d'impatto sulla protezione dei dati (DPIA).

Non è sempre facile valutare l'esistenza di rischi elevati. Tuttavia, una DPIA dovrebbe essere effettuata in ogni caso se i dati personali particolarmente sensibili sono trattati su larga scala. Tuttavia, questo non è il caso del trattamento dei dati dei dipendenti, anche se contengono dati personali che richiedono una protezione speciale.

Version 1.1|Italienisch |BU