AXA Fondazione
previdenza professionale

Previdenza professionale

Regolamento sulla protezione dati

AXA Fondazione previdenza professionale, Winterthur

L1287.003-09.23

Il presente regolamento per la protezione dati viene emanato dal consiglio di fondazione di AXA Fondazione previdenza professionale, Winterthur (di seguito «la fondazione»), sulla base del punto 2 dell'atto di fondazione e del punto 10 del vigente regolamento d'organizzazione.

Scopo

1

Collaboratrici e collaboratori, clienti, persone assicurate, beneficiari di prestazioni e altri soggetti, i cui dati personali vengono trattati dalla fondazione, si aspettano da essa una gestione responsabile e conforme alla legislazione vigente.

Ai fini del trattamento dei dati personali la fondazione si attiene al diritto applicabile e al presente regolamento sulla protezione dati. Il presente regolamento fornisce principi generali per la gestione dei dati personali ed è vincolante per tutti gli organi della fondazione, nonché per le collaboratrici e i collaboratori delegati o direttamente impiegati presso la fondazione (di seguito «**i collaboratori**»).

Quadro giuridico

2

La gestione dei dati personali si fonda in particolare sulle seguenti fonti normative:
- legge federale sulla protezione dei dati (LPD) con relativa ordinanza
- legge federale sulla previdenza professionale per la vecchiaia, i superstiti e l'invalidità (LPP) e relative ordinanze
- legge federale sul libero passaggio nella previdenza professionale per la vecchiaia, i superstiti e l'invalidità (LFLP) e relative ordinanze

Obbligo di riservatezza nell'ambito della previdenza professionale

3

Rientrano nell'obbligo di riservatezza tutte le informazioni sulle situazioni personali e finanziarie delle persone assicurate e dei datori di lavoro. Ai fini della comunicazione dei dati nell'ambito della previdenza professionale si applicano i requisiti specifici di cui all'art. 86a LPP.

Definizioni

4

In ambito di protezione dati hanno importanza fondamentale i concetti di dati personali e trattamento. Ogniqualvolta si sostanzi un caso di **trattamento di dati personali** occorre osservare le disposizioni in materia di privacy di cui al presente regolamento.

Dati personali
Sono considerati dati personali (di seguito «i dati») le informazioni relative a una persona fisica identificata o identificabile (di seguito «persona interessata»). Questi presuppongono un riferimento personale che diviene parzialmente chiaro solo nella situazione concreta. Al riguardo non ha alcuna rilevanza se i dati personali siano stati archiviati elettronicamente o salvati su un supporto fisico.

Sono dati personali ad esempio:
- dati di contatto come cognome, nome, recapito, indirizzo e-mail, numero telefonico
- informazioni su caratteristiche, comportamento, rendimento, condizione mentale, preferenze, qualità, opinioni e interazioni sociali, familiari o economiche
- dati identificativi come indirizzi IP, numero documento, numero AVS, numero assicurato o impronte digitali
- materiale audiovisivo con possibilità di risalire all'identità delle persone

Trattamento
In senso lato il concetto di trattamento dei dati personali descrive qualunque tipo di gestione di dette informazioni (su supporti elettronici o cartacei). Esempi:
- conservazione, memorizzazione e archiviazione
- raccolta/acquisizione
- accesso
- inoltro/trasmissione a terzi (ad esempio con l'utilizzo di una soluzione cloud o in caso di accesso ai dati da parte di un service provider esterno)
- elaborazione/analisi
- pubblicazione
- eliminazione/distruzione
- anonimizzazione/pseudonimizzazione

Il trattamento di dati personali online avviene in particolare tramite tracking tool, social media e cookie. Le applicazioni come le piattaforme di candidatura, ad esempio per le elezioni del consiglio di fondazione, conterranno in ogni caso dati personali. Ma il trattamento di informazioni si sostanzia anche con la conservazione dei fascicoli personali.

Dati personali degni di particolare protezione
Per il trattamento di dati personali che rientrano nella categoria (elenco esaustivo) delle informazioni degne di particolare protezione si applicano disposizioni più severe (cfr. di seguito).

I dati personali degni di particolare protezione riguardano:
- salute
- religione

– appartenenza etnica/razziale
– idee politiche/filosofiche
– sfera intima (orientamento/vita sessuale)
– opinioni o attività sindacali
– dati genetici/biometrici
– misure di assistenza sociale
– azioni penali/reati[1]

Profilazione
Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali informazioni per valutare determinati aspetti relativi a una persona fisica, in particolare per analizzare o prevedere il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, il luogo di soggiorno o gli spostamenti.

Profilazione con rischio elevato
Profilazione che comporta un rischio elevato per la personalità o i diritti fondamentali del la persona interessata, in quanto induce a collegare i dati consentendo una valutazione di aspetti fondamentali della personalità.

Principi
5

Equità
Il trattamento dei dati personali avviene secondo criteri di equità e soltanto nel modo in cui la persona interessata si può aspettare.

Trasparenza
Se i dati personali vengono acquisiti presso la persona interessata stessao o da altre fonti, questi viene informato attivamente, per tempo, in maniera dettagliata e comprensibile sul trattamento delle informazioni.

Limitazione delle finalità
I dati personali possono essere acquisiti solo per un determinato scopo, identificabile per la persona interessata, e trattati solo nella misura in cui questo sia compatibile con detto scopo (esempio: l'indirizzo e-mail fornito in un modulo di contatto non deve essere utilizzato per l'invio di una newsletter).

Minimizzazione dei dati
La raccolta di dati personali deve essere limitata a quanto strettamente necessario. Inoltre questi devono essere possibilmente anonimizzati o pseudonimizzati (esempio: per rispondere a una richiesta per un'offerta da parte di un broker che opera per un datore di lavoro, non è necessario fornire regolarmente nomi e cognomi degli assicurati).

Limiti di tempo per la conservazione
I dati personali possono essere salvati soltanto per quanto necessario per gli scopi perseguiti con il trattamento (esempio: un piano di eliminazione garantisce che i dati personali vengano cancellati alla scadenza di un determinato periodo).

Accuratezza
I dati personali devono essere esatti e mantenuti aggiornati.

Sicurezza
I dati personali devono essere trattati in maniera riservata e protetti con adeguate misure tecniche e organizzative da perdita, distruzione, modifica o divulgazione non autorizzate (esempi: verbalizzazione, codifica hardware di dispositivi mobili).

Basi giuridiche
I trattamenti dati presuppongono la presenza di una determinata base giuridica qualora si operi in violazione di uno dei principi di cui sopra, vengano comunicati a terzi dati personali degni di particolare protezione oppure il trattamento avvenga in contrasto con il consenso esplicito fornito dalla persona interessata.

Possono essere considerate basi giuridiche:
– disposizioni di legge (esempio: termini di conservazione legali per i giustificativi contabili)
– relazione diretta con la stipula o l'esecuzione di un contratto con la persona interessata dal trattamento dati
– nostro prevalente interesse al trattamento dati, se talmente importante da oltrepassare quello contrastante della persona interessata
– consenso della persona interessata

[1] incl. provvedimenti/sanzioni di tipo amministrativo.

Nell'ambito della previdenza professionale, in linea generale i dati personali possono essere elaborati soltanto a fronte di una base legale. Fanno eccezione le situazioni in cui la persona interessata, nel singolo caso, fornisce il proprio consenso al trattamento oppure rende accessibili i propri dati personali senza vietarne esplicitamente il trattamento. Il consenso deve essere esplicito per (i) ogni trattamento di dati personali degni di particolare protezione; (ii) una profilazione ad alto rischio nella previdenza extraobbligatoria; (iii) ogni profilazione nel campo della previdenza obbligatoria.

Non appena sorge il dubbio se sussista la base legale necessaria o sufficiente per un trattamento dati, ovvero se tale base legale sia richiesta, occorre consultare l'incaricato della protezione dati della fondazione.

Dichiarazione sulla protezione dei dati

6

Le persone interessate devono essere informate, in modo comprensibile e facilmente accessibile, sul trattamento dei loro dati personali, salvo tale procedura non sia prevista, ad esempio, per legge.

Le informazioni fornite alla persona interessata devono contenere perlomeno i seguenti dati:
- contatto del soggetto legale responsabile per i dati
- scopo del trattamento
- destinatari o categorie di destinatari
- indicazione degli stati destinatari, in caso di trasmissione all'estero
- categorie dati in caso di raccolta indiretta (non presso la persona interessata)
- modalità delle decisioni essenziali, assunte in maniera completamente automatica

Trattamento di dati personali su mandato

7

Il trattamento dei dati personali può essere demandato a un fornitore di servizi terzo, ma la fondazione resta responsabile nei confronti della persona interessata. Ai fini del coinvolgimento di un responsabile del trattamento dati su mandato devono essere soddisfatte le seguenti condizioni:
- il responsabile selezionato deve fornire garanzie sulla protezione e in particolare sulla sicurezza dei dati
- la trasmissione dei dati personali al responsabile del trattamento su mandato non deve violare gli obblighi di riservatezza previsti per legge o contratto
- prima di trasmettere i dati personali al responsabile del trattamento su mandato occorre stipulare, per iscritto o in altra forma testuale, un accordo specifico
- ove sia necessario incaricare un responsabile per il trattamento dati su mandato con sede all'estero, occorre inoltre che siano soddisfatte le condizioni di cui al punto 8

L'accordo deve prevedere, fra l'altro, l'obbligo per i responsabili del trattamento dati su mandato di elaborare le informazioni solamente in conformità con il proprio incarico e con le istruzioni della fondazione, le quali ne vietano l'utilizzo per altre finalità e impongono di garantire la sicurezza della gestione. I terzi incaricati possono essere coinvolti solo con il consenso della fondazione.

Trasmissione all'estero

8

I dati personali possono essere trasmessi all'estero solo se nello Stato destinatario sussiste un livello di protezione dati adeguato oppure se siano state adottate misure precauzionali di tutela come garanzie contrattuali.

Privacy by design: comunicazione di trattamenti dati nuovi, eliminati o sostanzialmente modificati

9

Per garantire la conformità della protezione dati di un processo, un'applicazione, un progetto o altra iniziativa e attivare le necessarie misure, la gestione operativa della fondazione deve coinvolgere quanto prima l'incaricato della protezione dati, compilando la lista di controllo per la valutazione d'impatto sulla protezione dei dati.

Esempi di trattamenti dati nuovi o sostanzialmente modificati possono essere:
- utilizzo di un nuovo software / una nuova applicazione o di relative determinate funzioni
- iniziative di marketing modificate
- analisi, elaborazione, associazione modificate o nuove di dati esistenti con riferimento personale
- utilizzo di software/applicazioni esistenti per la raccolta di ulteriori dati personali o per ulteriori scopi in aggiunta a quelli precedenti
- creazione di nuove raccolte dati
- concessione di un accesso remoto ai dati personali

Comunicazione di eventi critici

10

Le violazioni, sospette o effettive, della protezione dati devono essere comunicate al più presto e senza ulteriori ritardi al consulente per la protezione dati della fondazione (casistiche esemplificative: smartphone o notebook smarrito e non provvisto di codice di blocco, e-mail a destinatario errato). Il consulente per la protezione dati verifica la notifica ad autorità, persone interessate e altre misure.

L1287.003-09.23

Consulente per la protezione dei dati della fondazione:
Swiss Infosec AG
Centralstrasse 8A
6210 Sursee
Tel.: +41 (0)41 984 12 12
E-mail: datenschutzberater@infosec.ch

Trasmissione di richieste di persone interessate

11

Le richieste da parte di persone interessate e aventi per oggetto, ad esempio, accesso, rettifica, opposizione, trasferibilità dei dati o verifica di singole decisioni automatizzate, con riferimento ai loro dati personali, devono essere immediatamente inoltrate all'incaricato della protezione dati della fondazione, il quale predispone, fra l'altro, la raccolta intersettoriale delle informazioni e gestisce la comunicazione con le persone interessate stesse.

Organizzazione

12

Organi e collaboratori
Organi e collaboratori sono responsabili, entro le proprie aree di competenza e attività, per il rispetto dei principi fissati nel presente regolamento e la gestione dei dati personali.

Data owner
I data owner sono i principali responsabili per il rispetto della legislazione in materia di protezione dati e del presente regolamento, relativamente alla specifica raccolta dati ovvero allo specifico trattamento dati. Essi predispongono la relativa documentazione e, se necessario, l'esecuzione di una valutazione d'impatto sulla protezione dei dati.

IT
Il reparto IT adotta le necessarie misure tecniche e organizzative, entro la sfera dei sistemi informatici, per la tutela dei dati personali.

Incaricato della protezione dei dati
L'incaricato della protezione dati della fondazione ha il compito di fornire consulenza indipendente e coordinare il rispetto della protezione dati in tutta l'organizzazione. A tal riguardo questi necessita di un flusso di informazioni continuo e rapido da parte di tutti gli organi e i collaboratori, poiché per ottemperare a determinati obblighi di protezione dati occorre osservare termini cogenti.

L'incaricato della protezione dati coadiuva l'esecuzione di una valutazione d'impatto sulla protezione dei dati prevista per legge, fornisce consulenza sulla gestione dell'elenco delle attività di trattamento e sulla stesura del regolamento in materia, coordina la comunicazione di eventi critici e l'esercizio dei diritti delle persone interessate. Verifica, inoltre, se le persone interessate ricevano sufficienti informazioni in caso di trattamento dei loro dati. Ove necessario, questi formula e aggiorna le indicazioni in materia di protezione dati.

Sanzioni

13

Le violazioni al presente regolamento possono comportare provvedimenti disciplinari, civilistici o penali.

Disposizioni finali

14

Il presente regolamento può essere integrato da altre disposizioni o regolamenti riguardanti la gestione dei dati personali (ad es. direttiva sull'utilizzo di sistemi IT) ed entra in vigore il 1° settembre 2023.

L1287.003-09.23