PPF Group

Policy di protezione dei dati

CONTENUTO

Introduzione

Le regole di protezione dei dati dell'UE stanno cambiando con un nuovo quadro normativo. Il regolamento generale sulla protezione dei dati (GDPR) verrà rivisitato con la modificazione di requisiti di protezione dei dati e con l'introduzione di diritti più significativi per gli interessati, nuovi obblighi di responsabilità per le aziende e restrizioni continue sui trasferimenti internazionali di dati.

Con un focus sulla responsabilità sociale, PPF Group si impegna a rispettare a livello internazionale le leggi sulla protezione dei dati. Questa policy di protezione dei dati ("Policy di protezione dei dati") si basa sui relativi principi globalmente accettati. La garanzia della protezione dei dati rappresenta la base delle relazioni commerciali affidabili. Il trattamento legale e corretto dei dati personali da parte di PPF Group è perciò estremamente importante per il successo della sua attività.

PPF Group ha bisogno di raccogliere dati personali sulle persone con cui collabora per svolgere le proprie attività. Tali persone includono dipendenti (presenti, passati e futuri), clienti, fornitori e altri contatti commerciali. Le informazioni includono fondamentalmente nome, indirizzo, indirizzo e-mail, per i dipendenti: data di nascita, numero di figli, stato civile, numero di previdenza sociale e codice fiscale, nome da nubile della madre, ecc, come richiesto dalla legge. Indipendentemente dal modo in cui vengono raccolti, registrati e utilizzati (ad esempio su un computer o altri supporti digitali, su carta o immagini) questi dati personali devono essere trattati correttamente per garantire il rispetto dei principi fondamentali della legge.

Questa politica di protezione dei dati si applica a tutte le società del gruppo PPF (ciascuna di esse: "PPF") e ai loro dipendenti. La politica di protezione dei dati si estende a tutti i trattamenti di dati personali. I dati anonimizzati, ad esempio per valutazioni statistiche o studi, non sono soggetti a questa politica di protezione dei dati.

La policy di protezione dei dati è composta dalle seguenti tre parti:

- **Principi chiave dei dati**: Il capitolo 2 descrive i principi di alto livello che PPF deve rispettare nel trattamento dei dati personali (ad esempio, limitazione delle finalità, minimizzazione dei dati, accuratezza ecc.)
- **Responsabilità**: PPF deve implementare misure per dimostrare la conformità su base continuativa. Questo è un nuovo requisito del GDPR. Nel capitolo 3 descriviamo le misure che PPF dovrà mettere in atto per diventare un'organizzazione responsabile della privacy (ad esempio, effettuare la formazione, tenere documentazione delle attività di trattamento, implementare una policy di protezione dei dati, ecc.)
- **Sanzioni:** uno dei cambiamenti chiave che il GDPR porterà sono le sanzioni che possono essere imposte in caso di violazione delle norme sulla protezione dei dati. Nel capitolo 4 spieghiamo le basi delle nuove sanzioni.

Questa policy di protezione dei dati comprende i principi di privacy dei dati accettati a livello internazionale senza sostituire le leggi nazionali esistenti. Essa integra le leggi nazionali sulla privacy dei dati e le policy nazionali sulla privacy. La legge nazionale pertinente e le policy sulla privacy avranno la precedenza nel caso in cui siano in conflitto con questa policy di protezione dei dati, o abbiano requisiti più severi rispetto alla presente policy di protezione dei dati. PPF è responsabile del rispetto della presente Policy di protezione dei dati e degli obblighi legali, tenendo conto delle regole di conflitto di cui sopra.

La conformità con la policy di protezione dei dati e le leggi applicabili sulla protezione dei dati sono verificate regolarmente con audit sulla protezione dei dati e altri controlli.

La direzione delle società del Gruppo PPF è responsabile del trattamento dei dati nella propria area di responsabilità. Pertanto, sono tenuti a garantire che i requisiti legali, e quelli contenuti nella policy di protezione dei dati, per la protezione dei dati siano soddisfatti. Il management ha la responsabilità di assicurare che le misure organizzative, HR e tecniche siano in atto in modo che ogni trattamento dei dati sia effettuato in conformità con le norme sulla protezione dei dati. Al fine di soddisfare questo requisito, il PPF Group esaminerà questi elementi annualmente per ogni azienda e, se necessario, modificherà le notifiche e i consensi di protezione dei dati degli interessati. La revisione è coordinata dal responsabile Data Privacy e dai responsabili HR a livello locale, coinvolgendo tutti i dipartimenti e i dipendenti interessati.

Il responsabile Data Privacy è a disposizione per rispondere a qualsiasi domanda riguardante il GDPR e il modo in cui PPF dovrà conformarsi alla presente politica di protezione dei dati. Se avete domande o dubbi, potete contattarci all'indirizzo dataprivacy@ppfeurope.com.

1. INTRODUZIONE

1.1. Quali sono le leggi sulla protezione dei dati e come vengono applicati?

Nelle aree in cui opera il gruppo PPF, le principali legge applicabili in relazione alla protezione dei dati sono:

- Norme legali locali sulla protezione dei dati
- Regolamento generale sulla protezione dei dati UE 679/2016 (GDPR) (applicabile dal 25 maggio 2018)

Le leggi sulla protezione dei dati si applicano quando si elaborano:

- dati personali interamente o parzialmente con mezzi automatizzati; o
- dati personali che fanno parte di un sistema di archiviazione (o quando i dati sono destinati a far parte di un sistema di archiviazione).

I termini chiave sono "dati personali", "trattamento", "mezzi automatizzati" e "sistema di archiviazione".

1.2. Cosa sono i dati personali?

I dati personali sono un concetto molto ampio (vedi inserto).

Anche se le informazioni non permettono di per sé di identificare l'individuo a cui si riferiscono, tali informazioni possono comunque qualificarsi come dati personali.

Questo è il caso, per esempio, quando le informazioni:

- vengono usate per valutare, trattare in un certo modo o influenzare lo status o il comportamento di un individuo; o
- può avere un impatto sui diritti e gli interessi di una persona.

I dati personali sono tutte le informazioni relative a una persona fisica identificata o identificabile che, da sole o in combinazione con altre informazioni, identificano un individuo specifico. Una persona è identificabile quando può essere identificata, direttamente o indirettamente, in particolare mediante riferimento a un identificatore come un nome, un numero di identificazione, dati relativi all'ubicazione, un identificatore online o a uno o più fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale persona fisica.

Se i dati personali sono stati codificati, pseudonimizzati o criptati, continuano a costituire dati personali nella maggior parte dei casi. I dati personali cessano di essere tali quando sono stati resi anonimi in modo tale che diventa tecnicamente impossibile collegare i dati resi anonimi alla persona sottostante.

I dati personali non si limitano ai dati relativi alla vita privata di un individuo (ad esempio l'indirizzo privato di una persona). I dati relativi alla vita professionale dell'individuo possono anche qualificarsi come dati personali (ad esempio il suo numero di telefono diretto in ufficio).

Esempi di informazioni che, a seconda delle circostanze, possono costituire dati personali includono:

- Dettagli dello stipendio e del conto bancario di un lavoratore contenuti in uno dei vostri sistemi informatici
- Un'e-mail relativo ad un episodio che coinvolge un determinato lavoratore
- Un quaderno del manager contenente informazioni su un lavoratore.

Esempi di informazioni che, a seconda delle circostanze, non costituiscono dati personali includono:

- Un rapporto sul successo comparativo di diverse campagne in cui non si tengono dettagli sugli individui
- Un rapporto sui risultati delle interviste in uscita dove tutte le risposte sono rese anonime e dove è impossibile risalire agli individui.

Alcune categorie di dati personali sensibili beneficiano di una protezione speciale. Questi dati personali sensibili comprendono i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, e il trattamento di dati genetici e biometrici allo scopo di identificare in modo univoco una persona fisica, dati relativi alla salute o dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica.

Un esempio di dati personali sensibili sarebbe il riferimento che un dipendente lavora a metà tempo per motivi medici a causa di un piede ferito.

Il trattamento di dati personali sensibili è generalmente vietato, tranne che in condizioni rigorose, ad esempio quando l'elaborazione è necessaria per gli interessi vitali di un individuo, l'individuo ha dato il suo consenso per il trattamento o se il trattamento è necessario per la difese legali.

L'allegato 1 di questa policy di protezione dei dati contiene un diagramma di flusso facile da usare per aiutarvi a determinare se i dati possono essere considerati dati personali.

Per **trattamento** si intende qualsiasi operazione o insieme di operazioni compiute su dati personali o su insiemi di dati personali, con o senza l'ausilio di mezzi automatizzati, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, l'interconnessione, la limitazione, la cancellazione o la distruzione.

1.3. In che cosa consiste il trattamento?

Il trattamento ha una definizione molto ampia (vedi inserto sopra)

La maggior parte delle azioni svolte con dati personali vengono definite come trattamento. Ad esempio:

- Mantenere i file del personale
- Monitoraggio CCTV (a meno che il CCTV operi in un'area non accessibile agli individui)
- Mantenere un database CRM con i dettagli delle persone di contatto dei clienti di PPF
- Invio di newsletter a indirizzi e-mail di individui (ad esempio janos.kovacs@company.com)
- Memorizzare dati personali su un server

1.4. Cosa si intende per "sistemi automatizzati" e "sistemi di archiviazione"?

Per mezzi automatizzati ci riferiamo principalmente ai sistemi informatici (server, reti, PC, laptop, tablet, smartphone, telecamere a circuito chiuso, ecc.)

Pertanto, ogni volta che si utilizza un sistema IT per trattare dei dati personali, questo costituirà un trattamento e le leggi sulla protezione dei dati saranno applicate. Tuttavia, le leggi sulla protezione dei dati si applicano anche se si utilizzano i dati personali in un sistema di archiviazione esclusivamente cartaceo.

Per esempio, un file intitolato "Congedo dei dipendenti" che contiene divisori alfabetici può costituire un sistema di archiviazione e le leggi sulla protezione dei dati saranno applicate a questo file.

Per **sistema di archiviazione** si intende qualsiasi insieme strutturato di dati personali accessibili secondo criteri specifici, siano essi centralizzati, decentralizzati o dispersi su base funzionale o geografica.

1.5. Chi controlla i dati personali?

Le leggi sulla protezione dei dati distinguono tra "controllori" e "processori".

Il responsabile del trattamento determina gli scopi e le modalità di trattamento dei dati personali. Può farlo da solo, congiuntamente o collaborando con altre organizzazioni. Ciò significa che il controllore ha il potere di decisionale per quanto riguarda il "perché" e il "come" vengono svolte le attività di trattamento dei dati.

Per determinare se si è un controllore è necessario accertare quale organizzazione decide:

- Di raccogliere i dati personali e la base legale per farlo;
- Quali dati personali raccogliere, cioè il contenuto dei dati;
- Lo scopo o gli scopi per cui i dati devono essere usati;
- Su quali individui raccogliere i dati;
- Se divulgare i dati, e se sì, a chi;
- Se si applicano i diritti di accesso soggettivo e di altri individui, cioè l'applicazione di esenzioni; e
- Per quanto tempo conservare i dati o se apportare modifiche non di routine ai dati.

Queste sono tutte decisioni che possono essere prese solo dal controllore come parte del suo controllo generale dell'operazione di trattamento dei dati.

In linea con i termini dell'accordo con il controllore e del suo contratto, un processore può decidere:

- Quali sistemi informatici o altri metodi usare per raccogliere i dati personali;
- Come conservare i dati personali;
- Il dettaglio della sicurezza che circonda i dati personali;
- I mezzi utilizzati per trasferire i dati personali da un'organizzazione all'altra;
- I mezzi utilizzati per recuperare i dati personali su alcuni individui;
- Il metodo per garantire il rispetto di un programma di conservazione; e
- I mezzi utilizzati per cancellare o eliminare i dati.

Queste liste non sono esaustive, ma illustrano le differenze tra il ruolo del controllore e quello dell'incaricato del trattamento. Illustrano che un processore ha la libertà di usare le sue conoscenze tecniche per decidere come eseguire certe attività per conto del controllore. Tuttavia, non può prendere nessuna delle decisioni generali, per esempio per cosa saranno usati i dati personali o qual è il contenuto dei dati. Tali decisioni devono essere prese solo dal controllore.

1.6. Perché la distinzione tra controllori e processori è importante?

Gli obblighi di protezione dei dati che si applicano ai controllori e ai processori non sono identici.

I controllori hanno spesso più obblighi ai sensi delle leggi sulla protezione dei dati rispetto ai processori. Per esempio, quando un processore rileva una violazione dei dati personali, il processore deve informare il controllore e il controllore deve a sua volta notificare la violazione alle autorità per la privacy (e talvolta anche alle persone interessate).

Inoltre, i controllori e i processori devono stipulare un accordo scritto che prevede che l'incaricato deve:

- Elaborare i dati solo su istruzioni del controllore;
- I dipendenti e i sub-processori dell'incaricato siano vincolati da un obbligo di riservatezza;
- Garantire che non condividerà i dati con terzi, tranne che con i sub-processori autorizzati dal responsabile del trattamento;
- Adottare tutte le misure tecniche e organizzative appropriate per garantire un livello di sicurezza adeguato al rischio;

- Ingaggiare un subprocessore solo se il controllore ha dato la sua previa autorizzazione scritta (specifica o generale), imponendo al subprocessore gli stessi obblighi di protezione dei dati applicabili processore;
- Assistere il controllore nel mantenere la sicurezza dei dati, di notificare gli incidenti relativi alla sicurezza dei dati, di gestire le richieste degli interessati e di effettuare valutazioni d'impatto sulla privacy;
- A scelta controllore, cancellare o restituire tutti i dati alla scadenza o alla cessazione dei servizi + cancellare le copie esistenti (a meno che il contraente non sia obbligato per legge a conservare i dati, nel qual caso il contraente non può conservare i dati più a lungo di quanto richiesto dalla legge); e
- Accettare qualsiasi controllo da parte del controllore per verificare la conformità dei contraenti con l'accordo e con gli obblighi legali del contraente di proteggere i dati.

Di solito PPF si qualifica come controllore quando utilizza i dati personali. Quando si condividono i dati personali con parti esterne (ad esempio, fornitori di servizi esterni), è necessario verificare se la terza parte agirà come controllore o come processore. In quest'ultimo caso, la parte esterna dovrebbe elaborare quei dati solo per vostro conto e dovrebbe concludere con PPF un accordo scritto che contenga determinate disposizioni sulla protezione dei dati.

Nel caso in cui PPF determini i mezzi del trattamento insieme a un altro responsabile del trattamento, deve essere messo in atto un accordo per determinare in modo trasparente le rispettive responsabilità riguardo agli obblighi di trattamento, anche nei confronti degli interessati e in particolare per quanto riguarda gli obblighi di informazione (vedere la sezione 2.3).

2. PRINCIPI CHIAVE DELLA PROTEZIONE DEI DATI

Ogni operazione di trattamento dei dati deve rispettare i seguenti principi chiave di protezione dei dati. I dati personali devono essere:

1. Trattati sulla base di un motivo legale (condizioni per il trattamento)
2. Trattati per scopi limitati (principio di limitazione delle finalità)
3. Trattati in modo trasparente nei confronti della persona interessata (principio di trasparenza)
4. Adeguati, pertinenti e limitati a ciò che è necessario in relazione alle finalità per cui sono trattati (principio di minimizzazione dei dati)
5. Accurati e, se necessario, aggiornati (principio di accuratezza)
6. Conservati non oltre il tempo necessario in relazione alle finalità per cui sono trattati e poi distrutti o resi anonimi (principio di limitazione della conservazione)
7. Trattati in linea con i diritti degli interessati
8. Trattati in modo sicuro e confidenziale (principio di integrità e riservatezza)
9. Trasferiti a destinatari al di fuori dell'UE solo se vengono soddisfatte determinate condizioni

Di seguito forniremo ulteriori spiegazioni per ciascuno di questi principi.

2.1. Condizioni per il trattamento

PPF può trattare i dati personali solo se una (o più) delle seguenti condizioni è stata soddisfatta:

- La persona a cui si riferiscono i dati personali ha acconsentito al trattamento;
- Il trattamento è necessario:
    - in relazione a un contratto che l'individuo ha stipulato; o
    - perché l'individuo ha chiesto a PPF di fare qualcosa per poter stipulare un contratto;

- Il trattamento è necessario a causa di un obbligo legale che si applica a PPF (diverso dagli obblighi derivanti da un contratto);
- Il trattamento è necessario per proteggere gli "interessi vitali" dell'individuo. Questa condizione si applica solo in caso di vita o di morte, come quando la storia medica di un individuo viene rivelata a un ospedale che lo cura dopo un grave incidente sul lavoro;
- Il trattamento è necessario per l'adempimento di un interesse pubblico o per l'esercizio dei pubblici poteri di cui è investito il controllore.
- Il trattamento è necessario per i legittimi interessi di PPF (o di qualsiasi terza parte a cui vengono comunicati i dati) e su tali interessi non prevalgono gli interessi o i diritti fondamentali delle persone i cui dati vengono trattati. (motivo del legittimo interesse)

Ulteriori indicazioni su ciascuno di questi motivi di trattamento possono essere trovate nell'allegato 2.

I motivi legali per il trattamento dei dati personali sensibili sono più severi. I dati personali sensibili possono infatti essere trattati principalmente se:

- L'interessato ha dato il consenso al trattamento; o

- Il trattamento è necessario per rispettare un obbligo legale.

2.2. Trattamento limitato allo scopo (principio di limitazione allo scopo)

I dati personali possono essere trattati solo per scopi specifici che sono stati notificati alla persona interessata quando i dati sono stati raccolti per la prima volta.

Ciò significa che i dati personali non devono essere raccolti per uno scopo e utilizzati per un altro. Se diventa necessario cambiare lo scopo per il quale i dati vengono trattati, dovrete informare la persona interessata del nuovo scopo prima che avvenga qualsiasi trattamento e potrebbe essere necessario ottenere il suo consenso preventivo.

2.3. Trattamento trasparente (principio di trasparenza)

Agli individui devono essere fornite alcune informazioni sul trattamento dei loro dati personali. Le informazioni che devono essere fornite sono determinate in base a se i dati personali sono stati ottenuti direttamente dagli individui.

Le informazioni devono essere fornite in modo conciso, trasparente, comprensibile e facilmente accessibile, in un linguaggio chiaro e semplice. PPF non può chiedere denaro per la fornitura delle informazioni.

La tabella seguente riassume le informazioni che devono essere fornite agli individui e in quale fase.

Quali informazioni devono essere forniti?	Dati ottenuti direttamente dall'individuo	Dati non ottenuti direttamente dall'individuo
Identità e dettagli del controllore e del responsabile della protezione dei dati (se nominato da PPF)	✓	✓
Scopo del trattamento e la base legale per il trattamento	✓	✓
Interessi legittimi del controllore o delle terze parti, dove applicabile	✓	✓

Quali informazioni devono essere forniti?	Dati ottenuti direttamente dall'individuo	Dati non ottenuti direttamente dall'individuo
Categorie di dati personali		
Qualsiasi categoria di riceventi dei dati personali		
Dettagli dei trasferimenti ad altri paese e garanzie di sicurezza		
Periodo di ritenzione o criteri utilizzati per stabilire il periodo di ritenzione		
L'esistenza dei diritti relativi ai dati personali (diritto di accesso, alla rettificazione, all'eliminazione, alla limitazione del trattamento dei dati personali etc.)		
Il diritto di ritirare il consenso in qualsiasi momento, se rilevante.		
Il diritto di presentare un reclamo all'autorità di supervisione.		
La fonte di provenienza dei dati personali e se provengono da fonti accessibili al pubblico.		
Se la fornitura di dati personali è parte di un requisito o obbligo legale o contrattuale e le possibili conseguenze della mancata fornitura dei dati personali		
L'esistenza di un processo decisionale automatizzato, compresa la profilazione e le informazioni su come vengono prese le decisioni, il significato e le conseguenze.		

La tabella sotto illustra quando PPF deve fornire queste informazioni.

	Dati ottenuti direttamente dall'individuo	Dati non ottenuti direttamente dall'individuo
Quando dovrebbero essere forniti le informazioni	Nel momento in cui sono stati ottenuti dall'individuo	• Entro un periodo ragionevole dall'ottenimento dei dati (entro un mese) • Se i dati sono utilizzati per comunicare con la persona, al più tardi, quando avviene la prima comunicazione; o • Se è prevista la divulgazione ad un altro destinatario, al più tardi, prima della divulgazione dei dati.

2.4. Adeguato, pertinente e limitato a ciò che è necessario in relazione agli scopi (principio di minimizzazione dei dati)

Il GDPR ti impone di assicurarti di raccogliere solo i dati personali di cui hai bisogno per gli scopi che hai specificato. Ti obbliga inoltre a garantire che vengano raccolti soltanto i dati personali necessari per lo scopo per cui sono stati raccolti.

Non devi tenere più dati personali di quelli di cui hai bisogno. Né i dati in vostro possesso devono includere dettagli irrilevanti.

Quando si tratta di dati personali sensibili, è particolarmente importante assicurarsi di raccogliere o conservare solo la quantità minima di informazioni necessarie.

Se hai bisogno di tenere informazioni particolari solo su alcuni individui, dovresti raccoglierle solo per quegli individui - è probabile che le informazioni siano eccessive e irrilevanti in relazione ad altre persone. Per esempio, un datore di lavoro possiede i dettagli dei gruppi sanguigni di tutti i suoi dipendenti. Alcuni di loro fanno un lavoro pericoloso e le informazioni sono necessarie in caso di incidente. Per il resto della forza lavoro, però, tali informazioni sono probabilmente irrilevanti ed eccessive.

Non si dovrebbero conservare dati personali nella remota possibilità che possano essere utili in futuro. Tuttavia, è lecito conservare informazioni per un evento prevedibile che potrebbe non verificarsi mai, come nell'esempio di cui sopra sui gruppi sanguigni.

2.5. Accurati e, se necessario, aggiornati (principio di accuratezza)

Il GDPR vi impone l'obbligo di garantire l'accuratezza dei dati personali che trattate. Deve anche essere mantenuto aggiornato, se necessario.

Per conformarsi a queste disposizioni si dovrebbe:

- adottare misure ragionevoli per garantire l'accuratezza di tutti i dati personali che ottieni;
- garantire che la fonte di qualsiasi dato personale sia chiara
- considerare attentamente qualsiasi contestazione dell'accuratezza delle informazioni; e
- considerare se è necessario aggiornare le informazioni.

2.5.1. Quando è che i dati sono "accurati" o "non accurati"

Il GDPR non definisce la parola "accurato", ma dice che i dati personali sono inaccurati se non sono corretti o fuorvianti su qualsiasi questione di fatto. Di solito sarà chiaro se le informazioni sono accurate o meno. Per esempio, se una persona ha cambiato casa da Budapest a Praga, una registrazione che mostra che attualmente vive a Budapest

è ovviamente imprecisa. Ma una registrazione che mostra che una volta viveva a Budapest rimane accurata, anche se non ci vive più. Bisogna sempre essere chiari su ciò che una registrazione è destinata a mostrare.

2.5.2. I dati personali devono sempre essere aggiornati?

Questo dipende dall'uso che viene fatto delle informazioni. Se le informazioni sono usate per uno scopo necessita di dati attuali, devono essere tenute aggiornate. Per esempio, la registrazione della busta paga del dipendente deve essere aggiornata quando c'è un aumento di stipendio.

In altre circostanze, sarà altrettanto ovvio quando le informazioni non devono essere aggiornate.

2.5.3. Che cosa sono i "passi ragionevoli"?

Questo dipenderà dalle circostanze e, in particolare, dalla natura dei dati personali e dall'uso che ne verrà fatto. Più è importante che i dati personali siano accurati, maggiore sarà lo sforzo che dovrete fare per garantirne l'accuratezza. Quindi, se userete i dati per prendere decisioni che possono influenzare significativamente l'individuo interessato o altri, dovrete fare uno sforzo maggiore per garantire l'accuratezza. Questo può significare che dovete ottenere una conferma indipendente che i dati siano accurati. Per esempio, la maggior parte dei datori di lavoro avrà bisogno di controllare i dettagli precisi dell'istruzione, delle qualifiche e dell'esperienza lavorativa dei candidati solo se fosse essenziale per quel particolare ruolo, quando avrebbero bisogno di ottenere una verifica autorevole.

2.6. Conservati non oltre il tempo necessario in relazione alle finalità per cui sono trattati e poi distrutti o resi anonimi (principio di limitazione della conservazione)

Il GDPR non stabilisce alcun periodo minimo o massimo specifico per la conservazione dei dati personali. Invece, dice che i dati personali trattati per qualsiasi scopo o finalità non devono essere conservati più a lungo di quanto sia necessario per quello scopo o quelle finalità.

In pratica, significa che dovrete

- rivedere la durata di conservazione dei dati personali;
- considerare lo scopo o gli scopi per cui detenete le informazioni nel decidere se (e per quanto tempo) conservarle;
- cancellare in modo sicuro le informazioni che non sono più necessarie per questo o questi scopi; e
- aggiornare, archiviare o cancellare in modo sicuro le informazioni se non sono più attuali.

2.7. Trattati rispettando i diritti degli interessati.

Gli individui hanno un numero di diritti quando i loro dati personali vengono trattati.

2.7.1. Il diritto di essere informati

Vedere capitolo 2.3.

2.7.2. Il diritto di accedere ai dati personali

Gli individui hanno il diritto di ottenere:

- La conferma del trattamento dei loro dati;
- L'accesso ai loro dati personali; e
- Altre informazioni supplementari - questo corrisponde in gran parte alle informazioni che dovrebbero essere fornite nella notifica sulla privacy (vedi capitolo 2.3).

PPF deve fornire una copia di queste informazioni gratuitamente. Ma PPF può addebitare una "tassa ragionevole":

- Quando una richiesta è manifestamente infondata o eccessiva, in particolare se è ripetitiva; o
- Per soddisfare le richieste di ulteriori copie delle stesse informazioni. Questo non significa che potete far pagare tutte le richieste di accesso successive.

Quando ricevete una richiesta di accesso, dovrete fornire le informazioni richieste senza indugio e al più tardi entro un mese dal ricevimento.

Se le richieste sono manifestamente infondate o eccessive, in particolare perché sono ripetitive, PPF può:

- Addebitare una tassa ragionevole che tenga conto dei costi amministrativi per fornire le informazioni; o
- rifiutarsi di rispondere. Quando si rifiuta di rispondere a una richiesta, è necessario spiegarne il motivo all'individuo, informandolo del suo diritto di presentare un reclamo all'autorità di controllo competente per la protezione dei dati e del suo diritto di avviare un procedimento legale. PPF deve fornire queste informazioni senza indebito ritardo e al più tardi entro un mese.

Quando si riceve una richiesta di accesso, la prima cosa da fare è verificare l'identità della persona che presenta la richiesta, ad esempio chiedendo all'interessato di fornire una copia scannerizzata della carta d'identità.

Se la richiesta venisse fatta elettronicamente, dovreste fornire le informazioni in un formato elettronico comunemente usato (ad esempio in formato Word, Excel, PDF).

2.7.3. Il diritto alla rettifica

Gli individui possono chiedere a PPF di rettificare i dati personali che PPF detiene su di loro se i dati sono inesatti o incompleti. Se un individuo richiede a PPF di rettificare i suoi dati personali e se PPF ha divulgato i dati personali in questione a terzi (ad esempio l'età errata di un dirigente menzionato nella revisione annuale di PPF), PPF deve informare l'individuo:

- Della rettifica, se possibile; e
- Delle terze parti a cui i dati sono stati divulgati, se del caso.
- PPF deve rispondere entro un mese alle richieste di rettifica.

Se non intraprende azioni in risposta a una richiesta di rettifica, deve spiegarne il motivo all'individuo, informandolo del suo diritto di presentare un reclamo all'autorità di controllo competente per la protezione dei dati e del suo diritto di avviare un'azione legale.

2.7.4. Il diritto alla cancellazione

Il diritto alla cancellazione è noto anche come "diritto all'oblio". Il principio generale alla base di questo diritto è quello di consentire a un individuo di richiedere la cancellazione o la rimozione dei dati personali quando non vi è alcun motivo convincente per PPF di continuare a trattare i dati personali.

Il diritto alla cancellazione non fornisce un "diritto all'oblio" assoluto. Gli individui hanno il diritto di ottenere la cancellazione dei dati personali e di impedire il trattamento in circostanze specifiche:

- Quando i dati personali non sono più necessari in relazione allo scopo per il quale PPF ha originariamente raccolto/elaborato i dati;
- Quando l'individuo ritira il consenso;
- Quando l'individuo si oppone al trattamento e non esiste un interesse legittimo prevalente per PPF a continuare il trattamento dei dati personali;
- I dati personali sono stati elaborati illegalmente;
- I dati personali devono essere cancellati per rispettare un obbligo legale;
- I dati personali sono trattati in relazione all'offerta online di servizi o prodotti a un bambino.

Ci sono alcune circostanze specifiche in cui il diritto alla cancellazione non si applica e PPF può rifiutarsi di trattare una richiesta. Ad esempio, PPF può rifiutarsi di soddisfare una richiesta di cancellazione se i dati personali sono trattati per i seguenti motivi:

- Per adempiere a un obbligo legale (ad esempio, quando PPF deve elaborare i dati dei dipendenti per svolgere un compito che PPF è obbligato a svolgere in base a una legislazione locale di sicurezza sociale nella Repubblica Ceca, in Ungheria, nei Paesi Bassi, in Polonia, in Svezia, in Italia, in Germania);

- Per l'esecuzione di un compito di interesse pubblico o l'esercizio dei poteri ufficiali; o
- L'esercizio o la difesa di rivendicazioni legali.

2.7.5. Il diritto di limitare il trattamento dei dati

Gli individui possono chiedere a PPF di limitare il trattamento dei loro dati personali. Quando l'elaborazione è limitata, PPF è autorizzato a conservare i dati personali, ma non ad elaborarli ulteriormente. PPF può quindi conservare solo le informazioni sufficienti sull'individuo per garantire che la restrizione sia rispettata in futuro.

PPF sarà tenuta a limitare il trattamento dei dati personali nelle seguenti circostanze:

- Quando un individuo contesta l'accuratezza dei dati personali, PPF dovrà limitare il trattamento fino a quando non avrà verificato l'accuratezza dei dati personali;
- Quando un individuo si è opposto al trattamento (se il trattamento era necessario per l'esecuzione di un compito di interesse pubblico o scopo di interessi legittimi), e si sta valutando se i motivi legittimi di PPF prevalgono su quelli dell'individuo;
- Quando il trattamento è illegale e l'individuo si oppone alla cancellazione e richiede invece la limitazione;
- Se PPF non ha più bisogno dei dati personali ma l'individuo richiede i dati per stabilire, esercitare o difendere un diritto legale.

2.7.6. Il diritto alla portabilità

Il diritto alla portabilità dei dati permette agli individui di ottenere e riutilizzare i loro dati personali per i propri scopi attraverso diversi servizi. Permette loro di spostare, copiare o trasferire facilmente i dati personali da un ambiente informatico a un altro in modo sicuro e protetto, senza impedimenti alla fruibilità.

Il diritto alla portabilità dei dati si applica solo (ognuno dei seguenti tre criteri deve essere soddisfatto):

- Ai dati personali che un individuo ha fornito a un controllore;

- Quando il trattamento è basato sul consenso dell'individuo o per l'esecuzione di un contratto; e

- Quando il trattamento è effettuato con mezzi automatizzati.

Quando PPF riceve una richiesta di portabilità dei dati, PPF deve fornire i dati personali in un formato strutturato, comunemente usato e leggibile dalla macchina. I formati aperti includono file CSV, XML o JSON. Leggibile a macchina significa che le informazioni sono strutturate in modo che il software possa estrarre elementi specifici dei dati.

Se l'individuo lo richiede, PPF può essere tenuto a trasmettere i dati direttamente a un'altra organizzazione se ciò è tecnicamente fattibile. Tuttavia, PPF non è tenuto ad adottare o mantenere sistemi di elaborazione che siano tecnicamente compatibili con quelli di altre organizzazioni.

2.7.7. Diritto alla opposizione

Gli individui hanno il diritto di opporsi a:

- al trattamento basato su interessi legittimi o sull'esecuzione di un compito di interesse pubblico/esercizio dei pubblici poteri (compresa la profilazione);
- al marketing diretto (compresa la profilazione); e
- l'elaborazione a fini di ricerca scientifica/storica e statistica.

Come fa PPF a rispettare il diritto di opposizione?

> *i) Se PPF elabora i dati personali per l'esecuzione di un compito legale o per i legittimi interessi di PPF*

Gli individui devono avere un'obiezione per "motivi relativi alla sua situazione particolare". In questo caso, PPF deve interrompere il trattamento dei dati personali a meno che:

- Si possano dimostrare motivi legittimi significanti per il trattamento, che prevalgono sugli interessi, i diritti e le libertà dell'individuo; o
- L'elaborazione sia per l'istituzione, l'esercizio o la difesa di rivendicazioni legali.

PPF deve informare gli individui del loro diritto di opposizione al momento della prima comunicazione con l'individuo e nelle informative sulla privacy.

Questo deve essere esplicitamente portato all'attenzione dell'individuo e deve essere presentato chiaramente e separatamente da qualsiasi altra informazione fornita all'individuo.

ii) Se PPF tratta i dati personali per scopi di marketing diretto

PPF deve interrompere il trattamento dei dati personali per scopi di marketing diretto non appena si riceve un'obiezione. Non ci sono esenzioni o motivi per rifiutare.

PPF deve gestire immediatamente un'obiezione al trattamento per il marketing diretto in qualsiasi momento e gratuitamente.

PPF deve informare gli individui del loro diritto di opposizione al momento della prima comunicazione con l'individuo e nelle vostre informative sulla privacy.

Questo deve essere esplicitamente portato all'attenzione dell'individuo e deve essere presentato chiaramente e separatamente da qualsiasi altra informazione che fornite all'individuo.

2.7.8. Diritti relativi al processo decisionale automatizzato, compresa la profilazione

Le leggi sulla protezione dei dati proteggono gli individui dal rischio che una decisione potenzialmente dannosa sia presa senza alcun intervento umano.

Gli individui hanno il diritto di non essere soggetti a una decisione quando:

- La decisione è basata su un trattamento automatizzato; e
- produce un effetto legale o un effetto significativo simile sull'individuo.

Un esempio di quanto sopra potrebbe essere la situazione di un lavoratore il cui salario è direttamente collegato alla sua produttività e la sua produttività è misurata con mezzi completamente automatizzati.

Il PPF deve garantire che gli individui siano in grado di:

- Ottenere un intervento umano;
- Esprimere il loro punto di vista; e
- Ottenere una spiegazione della decisione e contestarla.

Questo diritto non si applica se la decisione:

- È necessaria per stipulare o eseguire un contratto tra PPF e l'individuo;
- È autorizzata dalla legge (ad esempio ai fini della prevenzione delle frodi o dell'evasione fiscale); o
- Si basa sul consenso esplicito.

Inoltre, il diritto non si applica quando una decisione non ha un effetto legale o un effetto altrettanto significativo su qualcuno.

Che cos'altro dice il GDPR sulla profilazione?

Le leggi sulla protezione dei dati limitano pure la "profilazione" degli individui. La profilazione è qualsiasi forma di trattamento automatizzato dei dati destinato a valutare alcuni aspetti personali di un individuo, in particolare per analizzare o prevedere elementi come ad esempio:

- Rendimento sul lavoro;

- Situazione economica;
- la salute;
- preferenze personali;
- Affidabilità; o
- Comportamento.

Quando si elaborano i dati personali per scopi di profilazione, PPF deve garantire che siano in atto garanzie appropriate. Tali salvaguardie includono almeno quanto segue:

- Fornire all'individuo informazioni significative sulla logica coinvolta, così come il significato e le conseguenze previste;
- Usare procedure matematiche o statistiche appropriate per la profilazione;
- Attuare misure tecniche e organizzative appropriate per consentire la correzione delle imprecisioni e ridurre al minimo il rischio di errori;
- Proteggere i dati personali in modo proporzionato al rischio per gli interessi e i diritti dell'individuo e prevenire effetti discriminatori.

Le decisioni automatizzate non devono essere basate sul trattamento di dati personali sensibili a meno che PPF non abbia ottenuto il consenso esplicito dell'individuo.

2.7.9. Modalità di gestione delle richieste degli interessati

Per ogni richiesta di una persona interessata relativa ai suoi diritti di accesso, rettifica, cancellazione, limitazione del trattamento e opposizione al trattamento dei suoi dati personali, nonché ai suoi diritti relativi alla portabilità dei dati e al processo decisionale automatizzato (compresa la profilazione) (vedere le sezioni da 2.7.2 a 2.7.8 sopra), devono essere seguite le seguenti linee guida:

- Le informazioni devono essere fornite per iscritto e, se del caso, per via elettronica;
- Le informazioni devono essere fornite senza indebito ritardo e in ogni caso entro un mese dalla richiesta;
- Se il periodo di un mese viene superato, e tenendo conto della complessità e del numero di richieste, questo periodo può essere esteso di altri due mesi, a condizione che l'interessato sia informato della proroga e dei motivi della stessa;
- Se PPF decide di non dare seguito a una richiesta, deve spiegare all'interessato i motivi di tale decisione senza indebito ritardo e in ogni caso entro un mese dalla richiesta;
- Le informazioni devono essere fornite gratuitamente all'interessato (tranne se la richiesta è manifestamente infondata o eccessiva, ad esempio per il suo carattere ripetitivo).

2.7.10. Notifica ai destinatari dei dati personali

Ogni volta che un interessato richiede a PPF di rettificare, cancellare o limitare il trattamento dei suoi dati personali (vedere le sezioni da 2.7.3 a 2.7.5 di cui sopra), deve comunicare la richiesta ai destinatari di tali dati personali, a meno che ciò sia impossibile o comporti uno sforzo sproporzionato.

Per esempio, su richiesta di un ex dipendente che chiede a PPF di cancellare i suoi dati personali, PPF deve inoltrare la richiesta a:

- La divisione contabile interna di PPF, se i dati personali sono elaborati attraverso un database contabile separato; e
- Un appaltatore terzo basato su cloud che fornisce servizi di risorse umane e/o buste paga a PPF.

PPF deve rendere accessibile l'elenco dei destinatari se l'interessato lo richiede.

2.8. Trattato in maniera sicura e confidenziale (principio di integrità e confidenzialità)

2.8.1. Obbligo di implementare misure di sicurezza

I dati personali sono soggetti alla segretezza dei dati. Qualsiasi raccolta, trattamento o utilizzo non autorizzato di tali dati da parte dei dipendenti è vietato. Qualsiasi trattamento di dati intrapreso da un dipendente che non era stato autorizzato a farlo nell'ambito dei suoi compiti legittimi non è autorizzata. I dipendenti possono avere accesso ai dati personali solo se appropriato al tipo e alla portata del compito in questione. Ai dipendenti è vietato utilizzare i dati personali per scopi privati o commerciali, rivelarli a persone non autorizzate o renderli disponibili in qualsiasi altro modo.

Il GDPR richiede di implementare misure tecniche e organizzative appropriate per garantire un livello di sicurezza adeguato al rischio che deriva dal trattamento (ad esempio distruzione accidentale o illegale, perdita, alterazione, divulgazione non autorizzata o accesso ai dati personali). Tali misure includono, ad esempio:

- La pseudonimizzazione e la crittografia dei dati personali;
- La capacità di garantire la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di elaborazione;
- La capacità di ripristinare la disponibilità e l'accesso ai dati personali in modo tempestivo in caso di incidente fisico o tecnico;
- Un processo per testare, esaminare e valutare regolarmente l'efficacia delle misure tecniche e organizzative per garantire la sicurezza del trattamento.

Questo obbligo rimane in vigore anche dopo la fine del rapporto di lavoro. Questo vale indipendentemente dal fatto che i dati siano trattati elettronicamente o in forma cartacea. Prima dell'introduzione di nuovi metodi di trattamento dei dati, in particolare di nuovi sistemi informatici, devono essere definite e implementate misure tecniche e organizzative per la protezione dei dati personali.

Quando sono appropriate le misure di sicurezza?

Il GDPR non fornisce linee guida dettagliate su quando le misure di sicurezza sono appropriate.

Si dovrebbe prendere in considerazione i seguenti criteri per determinare se le misure sono appropriate:

- Lo stato dell'arte della tecnologia e delle pratiche di sicurezza,
- I costi di implementazione delle misure
- La natura, la portata, il contesto e gli scopi del trattamento dei dati

2.8.2. Obbligo di segnalare le violazioni di dati personali

Che cos'è una violazione dei dati personali?

Qualsiasi violazione della sicurezza che porta alla distruzione, perdita, alterazione, divulgazione non autorizzata o accesso ai dati personali trasmessi, memorizzati o altrimenti elaborati da o per conto di PPF. Ciò significa che una violazione è più della semplice perdita di dati personali.

PPF deve segnalare alcuni tipi di violazione dei dati all'autorità di vigilanza competente per la protezione dei dati, e in alcuni casi anche alle persone interessate.

Ecco alcuni esempi di violazione dei dati:

- Perdita o furto di dati o di attrezzature su cui sono memorizzati i dati. Per esempio: prima di lasciare l'ufficio, un dipendente scarica su una chiavetta USB dei fogli di calcolo con i dati di contatto dei clienti (compresi nomi, indirizzi e-mail e numeri di telefono delle persone da contattare presso i vostri clienti). Quando arriva a casa si accorge di aver perso la chiavetta USB sul treno.
- Controlli di accesso inappropriati che permettono un uso non autorizzato. Per esempio: il dipartimento locale delle risorse umane ha memorizzato i documenti con i dati dei dipendenti (compresi i dati

salariali, ecc.) su un disco pubblico. Questi documenti erano disponibili a tutti i dipendenti PPF per due settimane. Almeno due dipendenti di PPF hanno avuto accesso ai dati e uno di loro ne ha preso una copia mentre stava lasciando l'azienda.

- Guasto alle attrezzature. Per esempio: i server di uno dei fornitori di servizi cloud esterni di PPF hanno subito un danno fisico che ha portato alla perdita di diversi dati personali dei dipendenti PPF.
- Errore umano. Per esempio: il vostro fornitore esterno di servizi di payroll ha inviato per errore documenti contenenti i dati dei dipendenti PPF (compresi i dati salariali, ecc.) a un altro cliente senza seguire la normale procedura di trasferimento dei dati.
- Attacco hacker ai vostri sistemi IT o ai sistemi IT gestiti da un fornitore di servizi esterno che gestisce i dati personali per vostro conto. Per esempio: un fornitore esterno di cloud che ospita il tuo database CRM è stato vittima di un attacco di hacking su larga scala.
- Attacco di spoofing in cui si ottengono informazioni ingannando l'utente. Per esempio: un dipendente viene ingannato cliccando sul link in una e-mail di spam che ha come risultato che l'intero database CRM viene copiato a distanza da un hacker.

PPF deve notificare all'autorità di controllo competente per la protezione dei dati una violazione che potrebbe comportare un rischio per i diritti e le libertà delle persone. Se non affrontata, una tale violazione può avere un effetto negativo significativo sugli individui - per esempio, risultare in discriminazione, danno alla reputazione, perdita finanziaria, perdita di riservatezza o qualsiasi altro svantaggio economico o sociale significativo.

Questo deve essere valutato caso per caso. Per esempio, PPF dovrà notificare all'autorità di vigilanza per la protezione dei dati competente la perdita dei dettagli dei clienti, se la violazione lascia gli individui esposti al furto di identità.

Inoltre, quando è probabile che una violazione comporti un rischio elevato per i diritti e le libertà degli individui, PPF deve notificare direttamente gli interessati. Un "rischio elevato" significa che la soglia per la notifica agli individui è più alta di quella per la notifica all'autorità di vigilanza competente.

Come notificare una violazione?

Se vieni a conoscenza di una violazione dei dati personali che può riguardare i dati personali trattati da o per conto di PPF, devi informare immediatamente il tuo manager e l'ufficio legale.

Le violazioni dei dati personali devono essere segnalate da PPF entro termini rigorosi (entro 72 ore alla competente autorità di vigilanza sulla protezione dei dati; senza indebito ritardo per gli individui interessati). Pertanto, è necessario segnalare qualsiasi violazione dei dati personali di cui si viene a conoscenza il prima possibile.

2.9. Trasferito a destinatari al di fuori dell'UE solo se vengono soddisfatte certe condizioni

2.9.1. In che cosa consiste il trasferimento dei dati

Un trasferimento dei dati comprende:

- L'invio di dati personali da un paese ad una persona in un altro paese (per esempio: un filiale in Ungheria invia dati HR a PPF nei paesi bassi); o
- Permettere ad una persona di un paese di accedere a dati personali archiviati in un altro paese. (esempio: PPF permette a un fornitore di servizi IT basato negli Stati Uniti di accedere remotamente a un database CRM in Ungheria per svolgere certe azioni con i dati.

2.9.2. Trasferimenti di dati nell'SEE

I dati personali possono essere trasferiti liberamente tra entità con sede nel SEE. Pertanto, è permesso che un'affiliata (ad esempio nella Repubblica Ceca, nei Paesi Bassi, in Polonia o in Slovacchia) invii i dati HR alla sede centrale della società in Ungheria (a condizione ovviamente che l'affiliata abbia rispettato i suoi altri obblighi di protezione dei dati).

2.9.3. Trasferimenti di dati dal UE a un destinatario al di fuori del SEE

Un controllore può trasferire i dati personali solo a paesi al di fuori del SEE (paesi terzi) che forniscono un adeguato livello di protezione dei dati. Per decidere se un paese fornisce un livello adeguato di protezione dei dati, il controllore può basarsi sulle decisioni della Commissione UE. A determinate condizioni, la Commissione UE ha finora riconosciuto Andorra, Argentina, Canada, Isole Faroe, Guernsey, Israele, Isola di Man, Jersey, Nuova Zelanda, Svizzera, Uruguay come paesi che forniscono una protezione adeguata.

Se un paese terzo non fornisce un adeguato livello di protezione dei dati, il controllore non può trasferire i dati personali a qualsiasi persona stabilita in quel paese terzo (importatore di dati), tranne se:

- L'individuo ha dato il suo consenso esplicito al trasferimento proposto dopo essere stato informato dei possibili rischi di tali trasferimenti;
- Il trasferimento è necessario per l'esecuzione di un contratto tra l'individuo e l'organizzazione o per misure precontrattuali prese su richiesta dell'individuo;
- Il trasferimento è necessario per l'esecuzione di un contratto stipulato nell'interesse dell'individuo tra il controllore e un'altra persona;
- Il trasferimento è necessario per importanti motivi di interesse pubblico;
- Il trasferimento è necessario per l'istituzione, l'esercizio o la difesa di rivendicazioni legali. Lo scopo di questa esenzione è di facilitare, per esempio, un trasferimento di dati personali da un'entità di controllo stabilita nel SEE a un'entità di controllo stabilita negli Stati Uniti, quando tale trasferimento è necessario per consentire a quest'ultima entità di stabilire o esercitare un diritto legale o di difendersi da un diritto legale avviato da una terza parte. Si prega di notare che questa eccezione deve essere interpretata rigorosamente. Pertanto, questa eccezione non può giustificare il trasferimento sistematico di dati personali a un responsabile del trattamento stabilito negli Stati Uniti semplicemente a causa della possibilità che un giorno possa sorgere un'azione legale;
- Il trasferimento è necessario per proteggere gli interessi vitali della persona interessata o di altre persone, quando la persona interessata è fisicamente o legalmente incapace di dare il consenso;
- Il trasferimento è fatto da un registro che secondo il diritto locale (cioè nella Repubblica Ceca, in Ungheria, nei Paesi Bassi, in Polonia, in Slovacchia, in Svezia, in Italia, in Germania) o il diritto dell'UE è destinato a fornire informazioni al pubblico (e che è aperto alla consultazione del pubblico in generale o di coloro che possono dimostrare un legittimo interesse a consultare il registro);
- Il controllore e l'importatore di dati (che agisce a sua volta come controllore o processore per quanto riguarda i dati personali trasferiti) hanno stipulato un accordo che fornisce sufficienti garanzie contrattuali. Il 4 giugno 2021 la Commissione ha emanato clausole contrattuali standard aggiornate ai sensi del GDPR per i trasferimenti di dati da titolari o responsabili del trattamento nell'UE/SEE (o altrimenti soggetti al GDPR) a titolari o responsabili stabiliti al di fuori dell'UE/SEE (e non soggetti a il GDPR). Una copia delle clausole modello è disponibile sul sito web della Commissione UE.
- All'interno di un gruppo aziendale, si può anche fare uso di impegni unilaterali (le cosiddette **regole aziendali vincolanti o BCR**). Le BCR sono una serie di regole vincolanti che possono essere messe in atto per consentire ai gruppi multinazionali di trasferire i dati personali che controllano dal SEE alle loro affiliate al di fuori del SEE in conformità con le leggi nazionali e dell'UE sulla protezione dei dati. Le BCR non coprono i trasferimenti di dati personali al di fuori di un gruppo aziendale.

Esistono altre esenzioni. Tuttavia, queste esenzioni sono meno rilevanti per PPF.

3. DIVENTARE RESPONSABILE IN TERMINI DI PRIVACY

3.1. Il principio di responsabilità

Il GDPR richiede alle aziende di diventare responsabili della privacy. Ciò significa che è responsabilità di PPF non solo conformarsi al GDPR, ma anche essere in grado di dimostrare, su base continuativa, che siete conformi.

Come si può dimostrare di essere conformi? Il GDPR richiede alle aziende di implementare misure tecniche e organizzative appropriate che assicurino e dimostrino la conformità:

- Adottare politiche interne di protezione dei dati (ad esempio la politica sulla privacy delle risorse umane)
- Organizzare sessioni di formazione sulla protezione dei dati per i membri del tuo staff che gestiscono dati personali
- Condurre audit interni sulle attività di trattamento
- Mantenere la documentazione pertinente sulle attività di trattamento
- Se appropriato e richiesto, nominare un responsabile della protezione dei dati
- Implementare misure che soddisfino i principi della protezione dei dati per design e della protezione dei dati per impostazione predefinita. Le misure potrebbero includere:
    - Minimizzazione dei dati;
    - Pseudonimizzazione;
    - Trasparenza; e
    - Creazione e miglioramento continuo delle caratteristiche di sicurezza.
- Utilizzare valutazioni d'impatto sulla protezione dei dati dove appropriato e richiesto.

Di seguito troverete ulteriori informazioni su alcune delle misure menzionate sopra.

3.2. Documentare le attività di trattamento

PPF è obbligato a mantenere registri interni delle sue attività di trattamento dei dati.

I registri interni devono contenere le seguenti informazioni:

- Nome e dettagli di PPF (e, se del caso, di altri controllori) e del responsabile della protezione dei dati.
- I vari scopi per cui PPF tratta i dati personali.
- Descrizione delle categorie di individui e delle categorie di dati personali che PPF tratta.
- Categorie di destinatari con cui PPF condivide i dati personali (ad esempio, fornitori esterni di servizi IT; fornitori esterni di servizi relativi alle risorse umane (cacciatori di teste, società di ricerca e selezione, ecc.)).
- Dettagli dei trasferimenti a paesi terzi, compresa la documentazione delle garanzie del meccanismo di trasferimento in atto (ad esempio l'uso di clausole modello).
- Programmi di conservazione dei dati.
- Descrizione delle misure di sicurezza tecniche e organizzative per proteggere i dati.

PPF può essere tenuta a mettere questi registri a disposizione dell'autorità di controllo della protezione dei dati competente ai fini di un'indagine.

3.3. Privacy by design e privacy by default.

Privacy by design significa che, in ogni fase dello sviluppo di un nuovo sistema o processo che utilizzerà dati personali (e durante l'intero ciclo di vita del trattamento dei dati), è necessario incorporare adeguate garanzie di privacy (come la pseudonimizzazione e la minimizzazione dei dati).

I seguenti criteri devono essere presi in considerazione per determinare ciò che è "appropriato":

- Lo stato dell'arte della tecnologia
- Il costo di implementazione delle garanzie

- La natura, la portata, il contesto e gli scopi del trattamento dei dati. Per esempio, quando un nuovo sistema è destinato a trattare dati personali su larga scala, le salvaguardie per la privacy dovranno essere più severe e protettive che se il trattamento fosse di scala più limitata.
- I rischi per gli individui che possono derivare dal trattamento. Per esempio, quando un nuovo sistema è destinato a trattare dati personali sensibili su un individuo, le garanzie di privacy dovranno essere più severe e più protettive che se il trattamento dei dati del nuovo sistema fosse meno invasivo.

Privacy by default significa che quando un sistema fornisce all'utente una scelta rispetto al trattamento dei suoi dati e l'individuo non intraprende alcuna azione per esprimere una preferenza, per default il sistema tratterà i dati personali nel modo meno invasivo per la privacy. Questo obbligo si applica alla quantità di dati personali raccolti attraverso il sistema, la portata del loro trattamento, il periodo della loro conservazione e la loro accessibilità.

3.4. Valutazioni d'impatto sulla protezione dei dati

Le valutazioni d'impatto sulla protezione dei dati (**DPIA**) (note anche come valutazioni d'impatto sulla privacy o PIA) sono uno strumento che può aiutare PPF a identificare il modo più efficace per rispettare gli obblighi di protezione dei dati e soddisfare le aspettative di privacy degli individui. Una DPIA efficace permetterà a PPF di identificare e risolvere i problemi in una fase iniziale, riducendo i costi associati e i danni alla reputazione che potrebbero altrimenti verificarsi.

PPF deve effettuare una DPIA quando:

- Si utilizzano nuove tecnologie; e
- È probabile che l'elaborazione comporti un rischio elevato per i diritti e le libertà degli individui. Ecco alcuni esempi di trattamento ad alto rischio:
    - Valutazione sistematica ed estesa degli individui che si basano su un trattamento automatizzato e che sono utilizzati per prendere decisioni che hanno effetti legali (o un effetto significativo simile sull'individuo);
    - Trattamento su larga scala di dati personali sensibili (ad esempio dati medici o dati personali relativi a condanne penali o reati);
    - Monitoraggio sistematico su larga scala di aree pubbliche (CCTV).

Ogni DPIA deve contenere:

- Una descrizione delle operazioni di trattamento e delle finalità, compresi, se del caso, i legittimi interessi perseguiti dal responsabile del trattamento;
- Una valutazione della necessità e proporzionalità del trattamento in relazione allo scopo;
- Una valutazione dei rischi per gli individui; e
- Le misure in atto per mitigare i rischi per gli individui, comprese le misure di sicurezza, e per dimostrare la conformità con le leggi sulla protezione dei dati.

4. CHE COSA SUCCEDE SE NON RISPETTI LE REGOLE?

A partire dal 25 maggio 2018, il livello delle sanzioni monetarie è significativamente più alto. Ci sarà un sistema a due livelli di multe amministrative, che sarà applicabile sia ai controllori che ai processori.

Alcune violazioni (ad esempio le disposizioni relative alla conservazione dei registri di trattamento - si veda la sezione 3.2) sono soggette a multe fino a 10.000.000 di euro, o fino al 2% del fatturato annuo mondiale di PPF nell'anno finanziario precedente (viene scelto il valore più alto tra le due).

Altre violazioni (come la violazione delle condizioni per il trattamento/condizioni per l'ottenimento del consenso) sono punibili con multe più alte, fino a EUR 20.000.000, o fino al 4% del fatturato annuo mondiale di PPF nell'anno finanziario precedente (viene scelto il valore più alto tra le due).

In termini di altri tipi di applicazione da parte delle autorità di protezione dei dati, anche questo è qualcosa che attualmente varia notevolmente tra gli Stati membri dell'UE ai sensi delle attuali leggi sulla protezione dei dati. Le

autorità per la protezione dei dati hanno poteri d'intervento, come il rilascio di pareri prima che il trattamento venga eseguito, e per ordinare il blocco, la cancellazione e la distruzione dei dati. Le autorità di protezione dei dati possono anche condurre audit e intentare azioni penali per violazioni del GDPR. I poteri di applicazione saranno, in generale, armonizzati sotto il GDPR (anche se l'applicazione penale è delegata agli Stati membri dell'UE). Essi includono il potere di emettere avvertimenti, richiami e ordini ai controllori e ai responsabili del trattamento; di imporre divieti temporanei e definitivi sul trattamento; di sospendere i flussi di dati all'estero; e di ordinare la rettifica o la cancellazione dei dati personali.

I tribunali possono ordinare:

- La confiscazione di tutti i supporti che contengono dati personali che sono stati trattati;
- La cancellazione di qualsiasi dato personale o può vietare a PPF di trattare qualsiasi dato personale
- Responsabilità civile per i danni causati dalla violazione degli obblighi di protezione dei dati.

I media possono anche pubblicare qualsiasi inosservanza della protezione dei dati che possa essere rilevante per il pubblico.

5. Approvazione, periodo di revisione, monitoraggio

La presente Policy è stata rivista, discussa e approvata dal Comitato esecutivo di PPF. La Policy dovrebbe essere rivista e aggiornata regolarmente, almeno una volta all'anno.

In caso di violazione della Policy, PPF utilizzerà tutti i mezzi per eliminare le condotte contrarie e intraprenderà le necessarie azioni legali e disciplinari, consentite dai rispettivi ordinamenti giuridici.

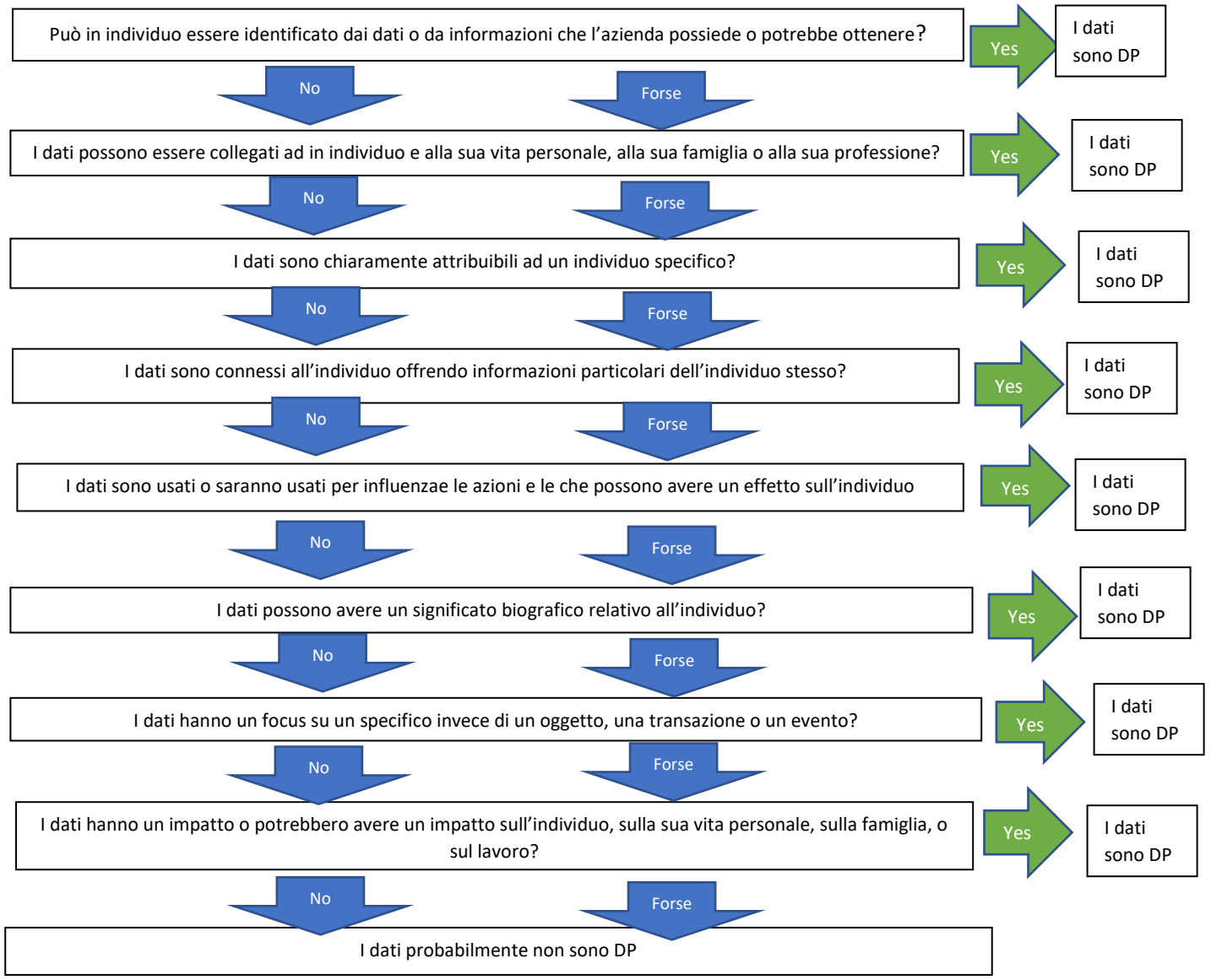
GERALD KÜHR
CEO

MARIEKE HOORNEMAN
CHIEF PEOPLE OFFICER

STÉPHANE RE
CFO

TORSTEN JACOBS
COO

ALLEGATO 1 – FLOWCHART – COSA SONO I DATI PERSONALI (DP)?



Collegati = dati che identificano un individuo, anche senza indicare il nome.

Chiaramente attribuibili = per esempio la storia medica, record criminale, record della performance al lavoro.

Esempio: se un dipendente ha una posizione unica nell'azienda, informazioni relative allo stipendio di quella persona sono considerati DP legati a quel dipendente.

Esempio: quando un dirigente partecipa ad una riunione del consiglio, il suo nome e titolo sono considerati dati personali. Pero questo non vuol dire che il verbale del meeting rappresenta dati personali di tutti coloro che hanno partecipato

Esempio: quando si parla della idoneità di un individuo per una particolare posizione, la documentazione di queste discussioni sono considerate come dati personali dell'individuo.

ALLEGATO 2 – ULTERIORI INDICAZIONI SULLE CONDIZIONI DI TRATTAMENTO

Base legale per il trattamento dei dati personali (non dai personali sensibili)	Ulteriori indicazioni
Consenso dell'individuo	Il consenso deve essere un'indicazione liberamente data, specifica, informata e inequivocabile dei desideri dell'individuo. In altre parole, il consenso richiede una qualche forma di chiara azione affermativa. Il silenzio, le caselle premarcate o l'inattività non possono costituire un consenso. Il consenso deve essere verificabile. Questo significa che dovete tenere una qualche forma di registrazione di come e quando il consenso è stato dato. Dovete ottenere la dichiarazione di consenso per iscritto o elettronicamente ai fini della documentazione. Quando iniziate un rapporto di lavoro, potete elaborare i dati personali dei candidati su loro consenso. Se PP rifiuta il candidato, dovete cancellare i suoi dati nel rispetto del periodo di conservazione richiesto, a meno che il candidato non abbia accettato di rimanere in archivio per un futuro processo di selezione. Se durante la procedura di candidatura dovesse essere necessario raccogliere informazioni su un candidato da una terza parte, dovete osservare i requisiti delle leggi nazionali corrispondenti. In caso di dubbio, dovete ottenere il consenso del candidato. Gli individui hanno il diritto di ritirare il consenso in qualsiasi momento. Ricorda che puoi fare affidamento su basi legali alternative al consenso - per esempio, quando l'elaborazione è necessaria ai fini degli interessi legittimi di PPF o di una terza parte.
Il trattamento e necessario per la creazione di un contratto con l'individuo	Questo copre solo il trattamento che è strettamente necessario per l'esecuzione di un contratto. Solo perché il trattamento dei dati è legato al contratto, o previsto da qualche parte nei termini e condizioni del contratto, non significa necessariamente che il trattamento sia strettamente necessario per l'esecuzione di un contratto. Pertanto, la regola generale è: PPF può eseguire il contratto senza trattare i dati? Se la risposta è "sì", allora non è necessario per l'esecuzione del contratto. Nei rapporti di lavoro, PPF può trattare i dati personali se necessario per avviare, eseguire e terminare il contratto di lavoro. Per esempio, PPF deve conoscere i numeri di conto bancario dei suoi dipendenti per essere in grado di eseguire i

	suoi obblighi ai sensi dei contratti di lavoro che ha concluso con i suoi dipendenti. In altre parole, PPF non può adempiere agli obblighi derivanti da questi contratti di lavoro senza elaborare i numeri di conto corrente dei dipendenti. Nel rapporto di lavoro esistente, il trattamento dei dati deve sempre riguardare lo scopo del contratto di lavoro se non si applica nessuna delle circostanze per il trattamento dei dati autorizzati. PPF può elaborare i dati personali dei prospect, dei clienti e dei partner interessati al fine di stabilire, eseguire e terminare un contratto. Prima di un contratto - durante la fase di avvio del contratto - PPF può elaborare i dati personali per preparare offerte o ordini di acquisto o per soddisfare altre richieste del potenziale cliente che riguardano la conclusione del contratto. PPF può contattare i potenziali clienti durante il processo di preparazione del contratto utilizzando le informazioni che hanno fornito. PPF deve rispettare tutte le restrizioni richieste dai potenziali clienti. Ci deve essere un'autorizzazione legale per elaborare i dati personali che sono legati al rapporto di lavoro ma che non erano originariamente parte dell'esecuzione del contratto di lavoro. Questo può includere requisiti legali, regolamenti collettivi con i rappresentanti dei dipendenti, il consenso del dipendente o l'interesse legittimo dell'azienda.
Il trattamento è necessario a causa di un obbligo legale che si applica a PPF (diverso dagli obblighi derivanti da un contratto).	Questa istanza riguarda solo obblighi legali chiari e specifici ai sensi del diritto dell'UE, del diritto locale (nella Repubblica Ceca, in Ungheria, nei Paesi Bassi, in Polonia, in Slovacchia, in Svezia, in Italia, in Germania) o ai sensi delle leggi di un altro stato membro dell'UE. In caso di linee guida non vincolanti (per esempio da parte delle autorità di regolamentazione), o di un obbligo legale straniero (per esempio degli Stati Uniti), considerare se PPF può fare affidamento sul motivo del legittimo interesse.
Il trattamento è necessario per proteggere gli interessi vitali dell'individuo.	Questa condizione si applica solo in casi di vita o di morte, come quando la storia medica di un individuo viene rivelata a un ospedale che lo cura dopo un grave incidente sul lavoro.
Il trattamento è necessario per i legittimi interessi di PPF (o di qualsiasi terza parte a cui i dati vengono comunicati) e tali interessi non sono superati dagli interessi o dai diritti fondamentali delle persone i cui dati vengono trattati.	Se PPF non potrà fare affidamento su nessuno dei suddetti motivi legali per il trattamento dei dati (consenso, esecuzione di un contratto, obbligo legale, ecc.), considerare se PPF può fare affidamento sul motivo del legittimo interesse. Gli interessi legittimi sono generalmente di natura legale (ad esempio, la riscossione di crediti in sospeso) o commerciale (ad esempio, evitare violazioni del contratto). Vedere l'allegato 3 della presente politica di protezione dei dati per una lista di controllo per determinare se si può fare affidamento su questo motivo legale per il trattamento.

ALLEGATO 3 – QUANDO PUOI UTILIZZARE LA MOTIVAZIONE DEL LEGITTIMO INTERESSE?

I seguenti passi possono aiutarvi a valutare se PPF può fare affidamento sul motivo del legittimo interesse:

Fase 1 - verificare se il tuo interesse è:

- Conforme al diritto dell'UE, al diritto locale (cioè nella Repubblica Ceca, Ungheria, Paesi Bassi, Polonia, Slovacchia, Svezia, Italia, Germania) o al diritto di un altro stato membro dell'UE; e
- articolato in modo sufficientemente chiaro da permettere di effettuare il balancing test rispetto agli interessi e ai diritti fondamentali dell'individuo (cioè sufficientemente concreto); e
- Un interesse reale e presente (cioè non essere speculativo).

Fase 2 - considerare se ci sono altri mezzi, meno invasivi, per raggiungere lo stesso scopo e interesse.

Fase 3 - valutare se l'interesse del controllore è superato dai diritti fondamentali o dagli interessi degli individui. Nel condurre tale valutazione, considerare i seguenti elementi:

- Il possibile svantaggio per PPF (e/o per terzi) se il trattamento dei dati non avesse luogo
- La natura dei dati che si intende trattare (dati sensibili? dati "normali"?)
- Lo status dell'individuo (minore, dipendente, cliente, ecc.)
- Il modo in cui i dati saranno trattati (su larga scala, data mining, analisi avanzate, profilazione, divulgazione a un gran numero di persone o pubblicazione)
- Le ragionevoli aspettative dell'individuo
- Confrontare l'impatto del trattamento sull'individuo e confrontarlo con il beneficio atteso dal trattamento per PPF

Fase 4 - se l'interesse dell'individuo non è superiore all'interesse dell'individuo, implementare adeguate garanzie aggiuntive per regolare l'equilibrio degli interessi. Tali salvaguardie possono includere per esempio:

- Minimizzazione dei dati (ad esempio, rigorose limitazioni alla raccolta dei dati, o cancellazione immediata dei dati dopo l'uso)
- Misure tecniche e organizzative per garantire che i dati non possano essere utilizzati per intraprendere altre azioni nei confronti degli individui ("separazione funzionale")
- Ampio uso di tecniche di anonimizzazione, aggregazione dei dati, tecnologie di miglioramento della privacy, privacy by design
- Aumentare la trasparenza (cioè fornire informazioni dettagliate sul modo in cui PPF tratterà i dati; spiegare le ragioni per cui si ritiene che i propri interessi non siano prevalenti rispetto a quelli dell'individuo)
- Fornire un diritto incondizionato di opposizione (opt-out) al trattamento se tale diritto di opposizione non è previsto dalla legge applicabile sulla protezione dei dati

Dettagli per revisioni e aggiornamenti della Policy

Nome Policy:	Group Data Protection Policy
Versione numero:	V3
Entrata in vigore:	1 Novembre 2024
Autorizzata da:	Comitato Esecutivo PPF
Scopo:	Tutte le aziende del Gruppo PPF e i loro dipendenti
Ciclo di revisione:	Annual dalla data di entrata in vigore
Responsabilità della documentazione del ciclo di revisione:	Consulente Legale

Storia delle revisioni	
Data: 1 Agosto 2018 Approvata da:	Creazione della V1 della Group Data Protection Policy Comitato Esecutivo PPF
Data: 1 Agosto 2023 Approvata da:	Entrata in vigore della V2 della Group Data Protection Policy Comitato Esecutivo PPF
Data: 1 Novembre 2024 Approvata da:	Modifica al Chief People Officer (V3) Comitato Esecutivo PPF