Gruppo di Lavoro
SICUREZZA INFORMATICA
Assintel

dalla GDPR TEORIA alla PRATICA

Paola Generali & Diego Perini

Gruppo di Lavoro Sicurezza Informatica Assintel

Il passintelligente per il tuo business

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

PRIVACY BY DESIGN E BY DEFAULT: PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE DEI DATI PER IMPOSTAZIONE PREDEFINITA

Gruppo di Lavoro
SICUREZZA INFORMATICA
Assintel

QUANDO DEVO APPLICARE LA PRIVACY BY DESIGN E BY DEFAULT?

SEMPRE

Quando si progettano le componenti organizzative e tecnologiche di un nuovo trattamento di dati personali.

In occasione di significativi cambiamenti organizzativi e tecnologici dei trattamenti di dati personali.

La Privacy by Design e by Default è una «filosofia generale di approccio», da applicare a tutti i trattamenti di dati personali.

Ha una particolare rilevanza nei trattamenti di dati personali che possono avere impatti rilevanti sui diritti e sulle libertà degli interessati, in particolare quando l'Azienda deve realizzare una valutazione di impatto, nei casi previsti dall'Art. 35 del «GDPR» (es. dati sanitari, profilazioni, ecc.).

Per favorire una sua corretta applicazione è opportuno adottare metodologie (semplificate) di Project Management e Change Management (es. progetto strutturato in fasi, identificazione di adempimenti, ruoli e controlli, assegnazione di ruoli e responsabilità, trasparenza, ecc.), in coerenza con la dimensione aziendale, la complessità e criticità dei trattamenti di dati personali.

IN COSA CONSISTE LA PRIVACY BY DESIGN E BY DEFAULT?

Privacy by Design e by Default sono due concetti «complementari» che favoriscono la prevenzione di trattamenti «non conformi» ai Principi Privacy: in sintesi richiedono di individuare, già in fase di disegno dei processi e delle applicazioni informatiche, misure di protezione dei dati (organizzative e tecnologiche) idonee a garantire la sicurezza dei dati nel rispetto dei diritti e delle libertà degli interessati, tenendo conto della tipologia dei dati trattati e dei possibili rischi nei trattamenti**.**

Le misure di protezione dei dati individuate in fase di progettazione devono essere messe in pratica e collaudate prima dell'avvio del trattamento.

Privacy by Design Protezione dei dati fin dalla progettazione	Identificare e formalizzare, in fase di progettazione dei trattamenti (es. sviluppo di una nuova applicazione di e-commerce), le misure di protezione (organizzative e tecnologiche) più adeguate in relazione ai rischi.
Privacy by Default Protezione dei dati per impostazione predefinita	Applicare (per impostazione predefinita) , fin dai primi trattamenti, soluzioni che garantiscano che siano trattati solo i dati personali necessari per le finalità previste e per il periodo strettamente necessario, assicurando il livello di protezione dei dati personali identificati in fase di progettazione.

QUALI SONO GLI OUTPUT DELLA PRIVACY BY DESIGN E BY DEFAULT?

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

Le soluzioni di Privacy by Design e Default devono essere **riportate nella documentazione progettuale** relativa ai trattamenti considerati. Tale documentazione deve evidenziare già in fase di fattibilità e progettazione dei trattamenti le misure organizzative e tecnologiche da adottare in fase di realizzazione delle procedure organizzative e del software dedicato ai trattamenti automatizzati.

La documentazione deve essere **approvata dal Titolare del Trattamento e nota al DPO** (se presente) e deve essere **archiviata e aggiornata nel tempo,** per consentire eventuali futuri Audit.

In caso di **cambiamenti** nel tempo delle procedure e dei sistemi ICT dedicati ai trattamenti, le **soluzioni** di Privacy by Design e Privacy by Default devono essere **rivalidate.**

Argomento	Privacy by Design	Privacy by Default
Sistemi di videosorveglianza	Progettare e configurare il sistema in modo tale che le registrazioni vengano cancellate in automatico alla scadenza dei termini consentiti (max. 7 giorni).	Registrazioni automaticamente cancellate allo scadere dei termini.
Termine del periodo di conservazione dei dati previsto per i trattamenti	Progettare le configurazioni di applicazioni e sistemi in modo che i dati vengano automaticamente cancellati, alla scadenza dei termini, dalle banche dati aziendali, dai dispositivi (es. PC, smartphone, ecc.) e dai sistemi di back-up.	Predefinire le soluzioni che consentano, in automatico, di cancellare i dati alla scadenza dei termini.
Registrazione/elaborazione dei dati nei database	Separazione dei dati in data base distinti: uno con i dati personali anagrafici e gli altri con i dati «critici» (es. dati sanitari o dati a rischio elevato).	Predefinire i trattamenti ove applicare la «separazione dei dati».
Prevenzione attacchi ad applicazioni informatiche sul Web	Sviluppare il codice applicativo in modalità sicura facendo riferimento a standard di Application Security (es. OWASP).	Effettuare Vulnerability Assessment, Penetration Test e Code Review prima del rilascio in produzione e periodicamente in fase di esercizio.

CASE STUDY: progettazione e sviluppo di una piattaforma di e-commerce

Privacy by Design:

- la piattaforma dovrà essere dotata di un sistema di controllo accessi mediante Strong Authentication;
- i dati relativi ai pagamenti effettuati con carte di credito dovranno essere protetti tramite crittografia;
- dovranno essere definite le soluzioni di back up e Disaster Recovery;
- dovranno essere adottati standard di Application Security (es. OWASP).

Privacy by Default:

- la piattaforma deve essere configurata in modo da raccogliere dall'utente i soli dati necessari per gestire gli acquisti on-line, eventuali ulteriori informazioni (es. consenso a newsletter, altre informazioni riferibili alla persona, ecc.) saranno richieste con altre modalità, in coerenza con il principi di finalità e limitazione del trattamento;
- i dati sono cancellati automaticamente entro 5 anni dall'ultimo ordine, salvo quelli necessari per adempimenti fiscali;
- l'Informativa deve precisare la presenza di profilazioni;
- certificazione PCI/DSS per pagamenti con carte di credito;
- Vulnerability Assessment, Penetration Test e Code Review prima del rilascio in produzione, poi con frequenza annuale.

Gruppo di Lavoro SICUREZZA INFORMATICA Assintel

CHI DEVE REALIZZARE LA PRIVACY BY DESIGN E BY DEFAULT ?

La Privacy by Design e by Default
è un caposaldo del Regolamento unitamente alla «Accountability».

Tutte le soluzioni adottate in ottemperanza al Regolamento devono rispondere a tali caposaldi (es. organizzazione, processi, soluzioni tecnologiche, ecc.) e possono costituire una «comprova» della corretta impostazione del sistema di gestione della Privacy aziendale da parte del Titolare del Trattamento.

Il Titolare del Trattamento deve definire le «regole» da seguire in Azienda da parte dei **Responsabili interni del Trattamento** e dei **Responsabili dei Servizi Aziendali** (es. servizi informatici, organizzazione, ecc.) per assicurare che le soluzioni relative ai nuovi trattamenti siano correttamente progettate e realizzate.

Si suggerisce di formalizzare tali regole all'interno di un "**Modello GDPR**» aziendale, in un'apposita Linea Guida intitolata «Privacy by Design e Privacy by Default», che definisca ruoli e responsabilità.
IL DPO, se presente, gioca un ruolo fondamentale di supporto e di controllo.

INFORMATIVA E CONSENSO

COME DEVE ESSERE UN'INFORMATIVA?

CONCISA	• Un'informativa di 20 pagg non è necessariamente esaustiva • Non dobbiamo includere informazioni che non sono pertinenti con il reale trattamento solo per l'ansia di «metterci al riparo»
FACILMENTE ACCESSIBILE	• L'informativa deve essere facilmente reperibile, es. chi ha un sito web dovrebbe mettere un link chiaro e visibile
CON UN LINGUAGGIO SEMPLICE	• Dobbiamo adeguare il lessico a chi leggerà l'informativa, pensiamo all' «uomo comune» • Usiamo, dove possibile, delle icone che richiamino il concetto
TRASPARENTE	• Non mescoliamo il testo con le note legali (es. sia nei contratti sia sui siti web) • Non utilizziamo «potremmo» – «dovremmo»: diciamo chiaramente come saranno trattati i dati personali

COSA SCRIVERE NELL'INFORMATIVA?

Il GDPR definisce alcuni elementi che devono essere necessariamente contenuti in ogni Informativa.
Per la stesura dell'informativa possiamo seguire le seguenti sezioni:

Liceità e finalità del trattamento

Andranno indicate tutti i motivi (Finalità) per cui i dati personali dell'interessato sono trattati. Esempi:

- Gestire il rapporto contrattuale
- Promuovere l'attività commerciale per mezzo di newsletter
- Fare attività di benchmarking o analisi statistiche

Andrà indicata la ragione per cui il trattamento è da considerarsi **lecito**. Esempi:

- Esiste il consenso dell'interessato
- Il trattamento è necessario per adempiere al contratto o ad un obbligo di legge

Durata del trattamento

Andrà indicata la durata massima di conservazione dei dati. Ricordiamo che i dati dovranno essere trattati per il tempo strettamente necessario per adempiere alle finalità. Esempi:

- non possiamo inserire frasi tipo «fino a quando sarà necessario» o «fino a quando si sarà esaurita la finalità».
- La durata deve essere definita o definibile: «I dati saranno conservati per 10 anni dalla scadenza del rapporto contrattuale»

COSA SCRIVERE NELL'INFORMATIVA?

Comunicazione dei dati

Andranno indicati i soggetti ai quali vengono comunicati i dati o che hanno accesso a questi. Esempi:

- Indicare se i dati saranno comunicati a soggetti extra EU o a soggetti esterni al Titolare del Trattamento
- Indicare quali dati possono essere comunicati e per quali finalità: «a soggetti terzi con sede esclusivamente in EU per attività di recupero crediti»

Diritti dell'Interessato

- Andranno indicati in modo esplicito tutti i diritti dell'Interessato: trasparenza – informativa – accesso - rettifica – oblio – limitazione del trattamento – portabilità dei dati – opposizione al trattamento
- Andrà specificata la possibilità di presentare reclamo al Garante riportando i riferimenti: es. garante@gpdp.it
- Andrà indicata una mail o un contatto del Titolare del Trattamento al quale l'Interessato potrà rivolgersi per esercitare i propri diritti.

Titolare del Trattamento e DPO

- Andranno indicati tutti i dati del Titolare del Trattamento: ragione sociale – indirizzo – telefono – mail
- Se presente, andrà indicato anche il riferimento del DPO e come contattarlo

INFORMATIVA E CONSENSO

L’informativa e il consenso sono sempre obbligatori?

INFORMATIVA

SEMPRE!

- L’interessato deve sempre sapere in che modo i suoi dati vengono trattati dal Titolare
- L’Informativa può essere data anche in forma orale (sconsigliata)
- Deve essere data entro un tempo ragionevole (non oltre 1 mese dalla raccolta) – quando i dati non siano stati ottenuti presso l’Interessato – altrimenti immediatamente

CONSENSO

DIPENDE…

NON È NECESSARIO SE:

- il trattamento è limitato alle attività precontrattuali e contrattuali (es. se devo fare un’offerta non ho bisogno del consenso
- Il trattamento è necessario per assolvere ad obblighi di legge (es. attività relative al diritto del lavoro o sicurezza. I dati di un dipendente possono essere trasmessi agli istituti previdenziali senza consenso preventivo)

IL CONSENSO – ALCUNE DOMANDE COMUNI

Posso raccogliere il consenso online?	• Il consenso deve essere INEQUIVOCABILE: significa che è necessaria un'azione positiva. Es. posso utilizzare una casella da barrare on line, ma NON posso pre barrarla
Posso inserire il consenso all'interno del contratto?	• Posso farlo, ma devo presentarlo in modo chiaramente distinguibile e con un linguaggio semplice e chiaro. Deve essere identificabile e anche in questo caso devo compiere un'azione positiva
Posso prevedere un unico consenso che sia valido per tutte le attività?	• Attenzione! Il consenso deve essere dato per ogni singola finalità. Ciò significa che se con gli stessi dati personali compio attività diverse dovrò prevedere ad esempio una casella da barrare per ogni attività
Devo prevedere la possibilità di poter rifiutare il consenso?	• Il consenso per essere libero deve prevedere per l'Interessato la possibilità di rifiutare. Es. per le attività di marketing il consenso non potrà essere obbligatorio

N.B. il consenso raccolto va conservato.
Il Titolare del Trattamento deve essere in grado di DIMOSTRARE che l'Interessato ha effettivamente fornito il proprio consenso.

IL REGISTRO DEI TRATTAMENTI

QUANDO REDIGERLO? A COSA SERVE?

L’obbligo di redigere il Registro dei trattamenti, ai sensi dell’Art. 30 del GDPR non si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati o di dati personali relativi a condanne penali e a reati

QUALE DIFFERENZA TRA:

REGISTRO DEI TRATTAMENTI TENUTO IN QUALITA’ DI TITOLARE DEL TRATTAMENTO

In esso il Titolare tiene conto delle attività di trattamento svolte sotto la **propria responsabilità.**

REGISTRO DEI TRATTAMENTI TENUTO IN QUALITA’ DI RESPONSABILE DEL TRATTAMENTO

In esso il Responsabile tiene conto di tutte le categorie di attività relative al trattamento svolte **per conto** di un Titolare del trattamento.

LA MIA AZIENDA HA MENO DI 250 DIPENDENTI?
QUAL E’ LA CONVENIENZA A TENERE COMUNQUE UN REGISTRO DEI TRATTAMENTI?

E’ di fondamentale importanza raccogliere le informazioni necessarie per mappare le attività di trattamento che l’azienda svolge al fine di analizzare e verificare i trattamenti in termini di criticità e conformità. La tenuta di un Registro dei Dati Trattati consente di mappare i trattamenti e dimostrare la conformità degli stessi ai requisiti imposti dal Regolamento.

In cosa è di supporto la tenuta di un Registro ai sensi dell’art. 30 del GDPR?

- Dimostrazione del rispetto del principio di **ACCOUNTABILITY**;
- Chiara, completa ed esaustiva redazione delle **Informative** da rilasciare ai soggetti interessati;
- Idoneo strumento per recepire le necessarie informazioni per ottemperare all’obbligo di Notifica all’Autorità Garante in caso di **data breach**;
- Strumento idoneo a dimostrare il **rispetto di una precisa richiesta** da parte del Titolare del trattamento, in caso di attività di trattamento svolta per suo conto, in qualità di Responsabile esterno.

QUALI INFORMAZIONI DEVONO ESSERE RIPORTATE?

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

QUALI INFORMAZIONI CONTENGONO RISPETTIVAMENTE?

REGISTRO DEI TRATTAMENTI TENUTO IN QUALITA' DI TITOLARE DEL TRATTAMENTO

- Il nome e i dati di contatto del titolare del trattamento, nonchè ove presente del DPO;
- Le finalità del trattamento;
- Descrizione delle categorie di soggetti interessati e delle categorie di dati personali;
- Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- L'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;
- I termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- Una descrizione generale delle misure di sicurezza tecniche e organizzative.

REGISTRO DEI TRATTAMENTI TENUTO IN QUALITA' DI RESPONSABILE DEL TRATTAMENTO

- Il nome e i dati di contatto del responsabile del trattamento e di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, nonchè ove presente del DPO;
- Le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- L'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate, se effettuato un trasferimento dei dati;
- Una descrizione generale delle misure di sicurezza tecniche e organizzative.

Gruppo di Lavoro SICUREZZA INFORMATICA Assintel

COM'E' FATTO UN REGISTRO DELLE ATTIVITA'?

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

REGISTRO DEI TRATTAMENTI TENUTO IN QUALITA' DI TITOLARE DEL TRATTAMENTO

TITOLARE DEL TRATTAMENTO E':

Nome Azienda: _____

Indirizzo: _____

Contatti: _____

Data Protection Officer: _____

CATEGORIA DATI TRATTATI	SOGGETTI INTERESSATI	FINALITA' DEL TRATTAMENTO	DESTINATARI DEI DATI	TRASFERIMENTI EXTRA UE	TEMPI DI CONSERVAZIONE	MISURE DI SICUREZZA
Dati Anagrafici Dati idonei a rilevare lo stato di salute	Dipendenti	Gestione del rapporto di lavoro	Consulente del lavoro nominato Responsabile esterno del trattamento	/ Oppure Svizzera: Decisioni di adeguatezza	10 anni dalla cessazione del rapporto di lavoro	**Misure tecnologiche: crittografia del DB** **Misure organizzative: segregazione degli accessi ai dati ai soli soggetti autorizzati** **Misure fisiche: Accesso alla sala CED e ai locali in cui sono apresenti archivi tramite badge**

Gruppo di Lavoro Sicurezza Informatica Assintel

COM'E' FATTO UN REGISTRO DELLE ATTIVITA'?

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

REGISTRO DEI TRATTAMENTI TENUTO IN QUALITA' DI RESPONSABILE DEL TRATTAMENTO

RESPONSABILE DEL TRATTAMENTO

Nome Azienda: _____

Data Protection Officer: _____

TITOLARE DEL TRATTAMENTO	CATEGORIA DATI TRATTATI	SOGGETTI INTERESSATI	FINALITA' DEL TRATTAMENTO	DESTINATARI DEI DATI	TRASFERIMENTI EXTRA UE	TEMPI DI CONSERVAZIONE	MISURE DI SICUREZZA
Nome Cliente (Titolare)	Dati personali (es. Anagrafiche) Dati particolari(es. Dati sullo stato di salute) Dati Giudiziari (es. Casellario giudiziario)	Dipendenti Clienti Fornitori	Assistenza e Manutenzione sistemistica	Indicare se Subappalto del servizio	/	Indicare tempi individuati dal Titolare all'interno della lettera di Nomina a Responsabile Esterno	Misure tecnologiche: accesso da remoto tramite protocolli sicuri, con OTP Misure organizzative: segregazione degli accessi ai dati ai soli soggetti autorizzati Misure fisiche: Accesso alla sala CED tramite badge

Gruppo di Lavoro SICUREZZA INFORMATICA Assintel

IL RESPONSABILE DEL TRATTAMENTO

CHI E' IL RESPONSABILE DEL TRATTAMENTO?

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

Il Responsabile del Trattamento è la persona fisica o giuridica cui il Titolare del Trattamento attribuisce in tutto o in parte l'esecuzione di uno o più trattamenti.

COSA SI INTENDE PER ESECUZIONE DI UN TRATTAMENTO DA PARTE DEL RESPONSABILE?

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la:

- Raccolta
- Registrazione
- Organizzazione
- Strutturazione
- Conservazione
- Adattamento o la modifica
- Estrazione
- Consultazione
- Uso
- Comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione
- Raffronto o l'interconnessione
- Limitazione
- Cancellazione o la distruzione

QUALI CATEGORIE DI FORNITORI SONO DA CONSIDERARSI RESPONSABILE ESTERNO DEL TRATTAMENTO?

Non esiste una categoria di Fornitore individuata dal GDPR come «Responsabile del Trattamento». E' necessario valutare, sulla base del rapporto intercorrente con il Titolare, se l'attività eseguita dal Fornitore rientra nel concetto di «trattamento di dati personali».

Cosa tenere in considerazione?

Il Titolare del trattamento DEVE regolamentare la consultazione, la manipolazione (es. cancellazione, modifica) ovvero la trasmissione dei dati personali che ha messo a disposizione dei suoi fornitori, per l'erogazione del servizio specifico.

Ad esempio: un **Fornitore ICT** che effettua attività di Assistenza e Manutenzione dell'infrastruttura tecnologica di un Titolare è sicuramente un soggetto che, per erogare il servizio richiesto, ha quantomeno la possibilità di consultare dei dati archiviati nei sistemi del Titolare, ovvero di manipolarli secondo le richieste di quest'ultimo. Si pensi a un fornitore ICT che si occupa di effettuare i back up dei sistemi aziendali, e di conservarli per conto del suo cliente (Titolare).

DESIGNARE IL RESPONSABILE DEL TRATTAMENTO

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

COME SI DESIGNA UN SOGGETTO ALLA QUALITA' DI RESPONSABILE DEL TRATTAMENTO?

I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un **contratto** o da altro **atto giuridico**, che vincoli il Responsabile del trattamento al Titolare del trattamento e che stipuli:

- La materia disciplinata e la durata del trattamento;
- La natura e la finalità del trattamento;
- Il tipo di dati personali e le categorie di interessati;
- Gli obblighi e i diritti del titolare del trattamento.

QUALI OBBLIGHI NEI CONFRONTI DEL RESPONSABILE ESTERNO VANNO REGOLAMENTATI ALL'INTERNO DELL'ATTO?

- Trattare i dati personali eseguendo le istruzioni fornite dal titolare;
- Rendersi disponibile a Audit di verifica da parte del titolare del trattamento;
- Assicurare che le persone autorizzate a trattare i dati personali si siano impegnate a rispettare vincoli di riservatezza;
- Su richiesta del titolare cancellare o restituire i dati personali al termine del trattamento;
- Implementare e mantenere tutte le misure tecniche e organizzative adeguate;
- Fornire al titolare qualsiasi informazione necessaria per dimostrare il rispetto del Regolamento;
- Tenere un Registro delle categorie di attività di trattamento dei dati personali svolte per conto del Titolare del trattamento;
- Avvertire il titolare del trattamento immediatamente dopo aver riscontrato il verificarsi di una violazione dei dati;
- Assistere il titolare del trattamento per la gestione delle richieste di diritto d'accesso e per gli altri obblighi imposti dal Regolamento;
- Cooperare con l'Autorità di Vigilanza;
- Designare un Responsabile della Protezione dei Dati (DPO), nei casi in cui è richiesto

DESIGNAZIONE DEL RESPONSABILE DEL TRATTAMENTO

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

COSA FARE SE UN FORNITORE RIFIUTA L'ATTO DI DESIGNAZIONE ALLA QUALITA' DI RESPONSABILE DEL TRATTAMENTO?

Il GDPR sancisce: «il Titolare ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato»

Bisogna anzitutto chiedersi:

1. QUANTO E' IN COMPLIANCE CON IL GDPR UN FORNITORE CHE **NON SA** DI SVOLGERE UN'ATTIVITA' CHE COMPORTA UN TRATTAMENTO DI DATI PERSONALI DI CUI **NON E**' TITOLARE?
2. QUANTO E' IN COMPLIANCE CON IL GDPR UN TITOLARE CHE CONTINUA A COLLABORARE CON UN FORNITORE **CHE RIFIUTA** UNA NOMINA A RESPONSABILE DEL TRATTAMENTO?

CONTINUARE A COLLABORARE CON IL FORNITORE CHE NON ACCETTA LA NOMINA QUALI CONSEGUENZE DETERMINA?

Se il Titolare del trattamento si assume la piena responsabilità del trattamento effettuato dal fornitore, NON designato Responsabile, i Soggetti Interessati sono al sicuro da eventuali violazioni al GDPR eseguite da quest'ultimo e, quindi, da possibili conseguenze dannose?

NO!

Il Fornitore che non ha accettato la nomina effettua un Trattamento di dati illegittimo.

ALLORA QUAL E' IL SUO RUOLO?

- Titolare Autonomo del trattamento? se così fosse, il fornitore sarebbe il soggetto che determina le finalità e i mezzi del trattamento di dati personali. Tali specifiche sono invece determinate dal suo cliente (Titolare) che gli delega l'erogazione di un servizio. Se il fornitore fosse un Titolare autonomo dovrebbe rilasciare a ogni soggetto interessato una sua Informativa sul trattamento dei dati, completa dell'eventuale richiesta di consenso per finalità di trattamento specifiche (es. Trattamento dati particolari, finalità di marketing e profilazione).
- Responsabile del Trattameno «di fatto»? Tale figura non esiste ai sensi del GDPR, che prevede una designazione formale del Responsabile mediante apposito atto giuridico, predisposto dal Titolare autonomo.

COSA PUO' FARE IL TITOLARE IN QUESTO CASO?

- VALUTARE ATTENTAMENTE IL FORNITORE IN QUESTIONE
- INTERROMPERE LA COLLABORAZIONE E RIVOLGERSI A UN ALTRO FORNITORE CHE PRESENTI LE GARANZIE PREVISTE DAL GDPR E ACCETTI L'ATTO DI DESIGNAZIONE

ECCO ALCUNE DELLE VIOLAZIONI AL GDPR CHE VERREBBERO OTTEMPERATE:

- Violazione dei principi (Art. 5)
- Liceità del trattamento (Art. 6)
- Consenso al trattamento (Art. 7)
- Informativa (Art. 13)

Il GDPR prevede una Sanzione fino ad un massimo di 20.000.000 Euro o al 4% del fatturato mondiale totale annuo

DESIGNAZIONE DEL RESPONSABILE DEL TRATTAMENTO

COSA FARE SE UN FORNITORE PROPONE IL SUO TEMPLATE STANDARD DI (AUTO) DESIGNAZIONE ALLA QUALITA' DI RESPONSABILE DEL TRATTAMENTO?

Il GDPR dispone in capo al TITOLARE del trattamento l'obbligo di regolamentare e disciplinare il trattamento di dati svolto da un suo Responsabile del trattamento.
Tale onere **NON SPETTA** al Responsabile

1 **VALUTARE LA NOMINA PROPOSTA DAL FORNITORE**:
Quali garanzie assicura? E' prevista la redazione di un Registro in qualità di Responsabile?
C'è congruenza tra quanto disposto rispetto al servizio richiesto?
Le misure di sicurezza garantite sono soddisfacenti?
Il diritto di audit è garantito?
E in caso di data breach, entro quanto è in grado di comunicare un'eventuale violazione?
Cosa riporta in merito all'esercizio dei diritti degli interessati?
Cosa riporta in merito all'utilizzo di subfornitori? E sul trasferimento Extra UE?

2 **VALUTARE IL FORNITORE, ANCHE IN RELAZIONE AL POTERE CONTRATTUALE SUL MERCATO**

I fornitori «big» tendono oggi a proporre Data Protection Agreement (DPA) standard, seguendo la scia della contrattazione standard.
Tale attitudine è comprensibile alla luce della necessità di un fornitore di grandi dimensioni nel mercato, di gestire al meglio l'erogazione del suo servizio e il conseguente trattamento di dati personali in qualità di Responsabile per conto di una quantità di Titolari autonomi (suoi clienti) non facilmente quantificabile.
Il GDPR però non utilizza le medesime logiche.

Il TITOLARE del trattamento ha **SEMPRE** il diritto (in quanto SUO DOVERE) di trattare il DPA proposto dal fornitore «big», di rifiutarlo e **pretendere** l'utilizzo di un proprio DPA.

DPIA
Il Data Protection Impact Assessment

COS'E' LA DPIA?

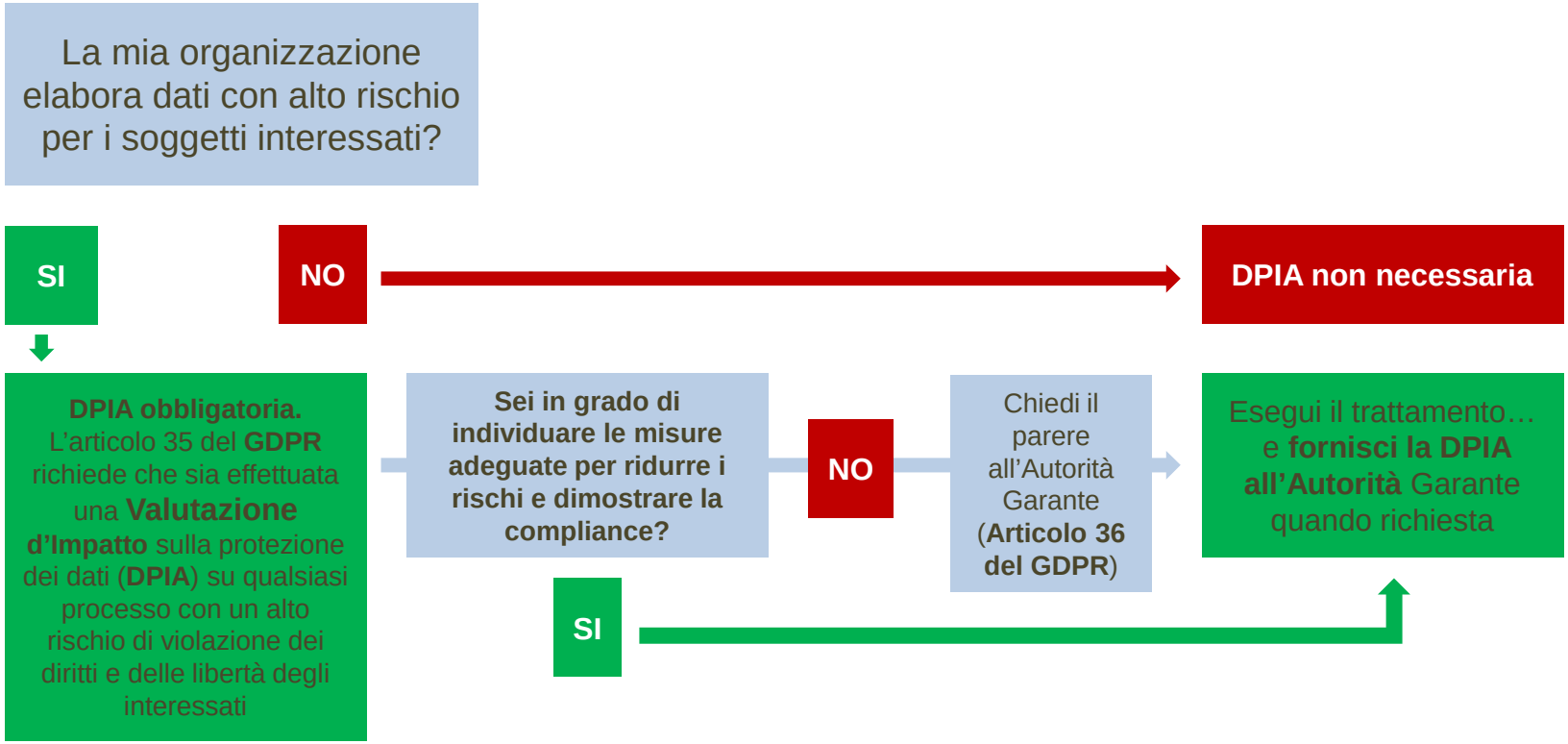
GDPR articolo 35: "valutazione d'impatto sulla protezione dei dati" o "data protection impact assesment" (cd. **"DPIA"**): è che un processo volto a descrivere:

- un trattamento di dati personali
- valutarne la necessità e la proporzionalità
- gestione dei rischi per i diritti e le libertà delle persone fisiche da esso derivanti,

effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo.

Il **DPIA** va inquadrato come uno strumento essenziale e fondamentale per tutti i titolari e responsabili del trattamento al fine di dar corso al nuovo approccio alla protezione dei dati personali voluto dal legislatore comunitario e fortemente basato sul principio della responsabilizzazione (cd. accountability principle).

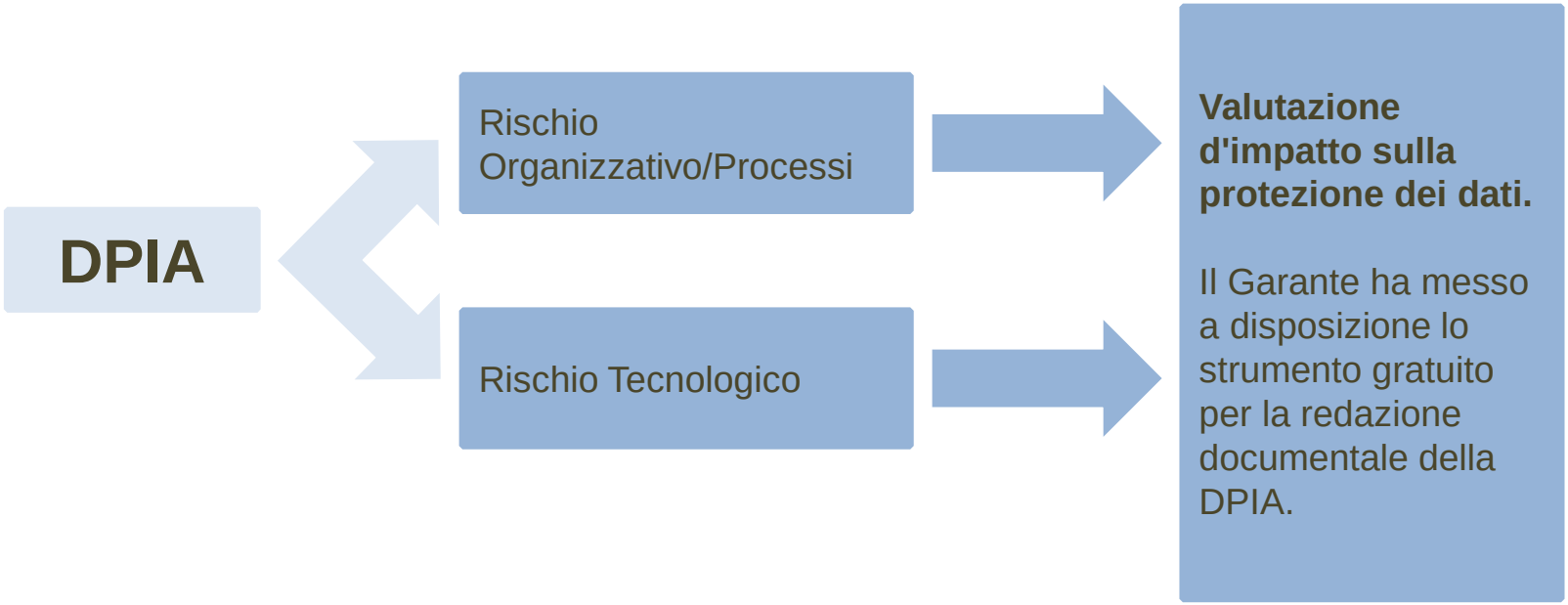
QUANDO E' OBBLIGATORIA?



QUANDO E' OBBLIGATORIA?

1. PASSO	**RISCHIO POTENZIALE LORDO** (cioè una valutazione senza considerare i controlli e le misure di sicurezza applicate). Andremo a individuare le tipologie e le quantità dei dati coinvolti nelle diverse attività di trattamento; in base a questi dati, per ogni trattamento, andremo ad individuare/definire i rischi potenziali, che potrebbero derivare agli interessati dalla perdita di sicurezza dei dati.	RISCHIO Lordo= **IMPATTO x Probabilità**
2. PASSO	**RISCHIO POTENZIALE NETTO**: In base alle misure di sicurezza applicate e ai controlli eseguiti nel trattamento, andremo a ridurre la probabilità/frequenza di accadimento e/o l'impatto per le varie tipologie di rischio analizzate. Con la stessa matrice sopra indicata calcoliamo quindi il **rischio effettivo netto** (cioè ridotto dalle contromisure di sicurezza applicate)	RISCHIO NETTO= **RISCHI LORDO-MISURE di Sicurezza**
3. PASSO	**ACCETTAZIONE DEL RISCHIO:** A questo punto dovremo individuare soluzioni tecniche e organizzative che consentano di ridurre gli eventuali rischi identificati o accettarli.	**Riduzione** dei **Rischi** o **Accettazione**

COME SI EFFETTUA LA DPIA?



QUALI SONO LE FASI DELLA DPIA?

ATTIVITA’	Rischio Organizzativo	Rischio Tecnologico
MAPPARE	Processi e Flussi organizzativi coinvolti nel ciclo di vita del dato	Asset Tecnologici coinvolti nel ciclo di vita del dato
IDENTIFICARE	Criticità e le minacce	Vulnerabilità
ANALISI	Impatti e Probabilità	Impatti e Probabilità
VALUTARE	Livelli di Rischio	Livelli di Rischio
Action Plan	Definizione del Piano di Azione e/o Accettazione	Definizione del Piano di Azione e/o Accettazione

MISURE DI SICUREZZA IDONEE

COSA SONO LE MISURE DI SICUREZZA IDONEE

Policy, procedure organizzative e misure tecniche da porre in atto se sono stati individuati **trattamenti di Dati Personali** suscettibili di generare dei **rischi elevati per i diritti e le libertà dei Soggetti Interessati**

Sono previste, direttamente o indirettamente, **in diversi articoli e considerata del GDPR.**

Cosa significa che devo implementare misure adeguate? Adeguate a cosa?

L'adozione di **misure di sicurezza** è prima di tutto **importante** per la **salvaguardia** dei dati aziendali, importanti a fini di **business**.

STRUMENTI IN PRATICA

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

Procedure organizzative

- **Formazione** e sensibilizzazione **addetti al trattamento**
- **Definizione ruoli e responsabilità** e relative nomine formali
- **Gestione** reclami e **richieste esercizio diritti**
- **Rispetto** del **principio** della **protezione** dei **dati** già in fase di progettazione di un'applicazione o di un trattamento e di default
- **Revisione** annuale **politica di sicurezza**
- Procedure per l'**assegnazione**, la **gestione** e la **revoca** di **diritti** e **responsabilità**
- Politica di **controllo degli accessi**
- Tenuta di un **registro delle risorse IT** utilizzate per il trattamento dei dati personali
- Predisporre un **piano di incident management**
- Definire **procedure** di gestione dei **data breach**
- Adozione di un **Business Continuity Plan**
- **Policy** di definizione e **gestione password**
- Definizione di **policy** per l'**identificazione** del **personale** e dei **visitatori** che accedono ai locali dell'organizzazione

Misure tecniche

- Soluzioni di **backup**
- Strumenti di **monitoraggio**
- Soluzioni di **gestione delle password**
- Sistemi di **log management**
- Cloud **Access Security Broker**
- Soluzioni di cifratura e **crittografia**
- **Antivirus** e detection signatures
- Strumenti di **patch management**
- **Firewall** e soluzioni di prevenzione e rilevamento intrusioni
- Servizi di **vulnerability assessment** e **penetration test**
- Dispositivi per la **distruzione** di **archivi** cartacei e supporti magnetici

Gruppo di Lavoro
SICUREZZA INFORMATICA
Assintel

QUALI STRUMENTI ADOTTARE?

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

CATEGORIA	STRUMENTI									
	Compliance	Application Access Control	Crittografia	Sistemi di audit	Firewall	Session timeout	Security Risk Assessment	Strumenti di monitoraggio e alerting	Replica dati e sistemi	Back up
Protezione dei dati		✓	✓		✓	✓				
Tutela Privacy / Riservatezza		✓	✓			✓				
Integrità dei dati		✓		✓				✓		✓
Cifratura / Anonimizzazione Pseudonimizzazione			✓							
Controllo Accessi / Protezione da danni accidentali o dolosi	✓	✓			✓	✓		✓		
Risk Assessment							✓			
Controllo Log e Auditing				✓	✓					
Security Settings And Policy	✓						✓		✓	
Business Continuity / Disaster Recovery									✓	
Back up / Restore										✓

Gruppo di Lavoro SICUREZZA INFORMATICA Assintel

QUALI STRUMENTI ADOTTARE?

Tipologia di strumenti per modalità di azione

ASSESSMENT	PREVENZIONE	HEALTH CHECK & DETECTION
Sensitive Data Discovery	Crittografia dei data base	Monitoring
Risk Assessment	Privileged Access Control	Alerting & Reporting
Security Assessment	Data Masking	Secure Configuration, Database Auditing
Privilege Analysis	Data Reduction	SQL Firewall

COME IMPLEMENTARE LE MISURE DI SICUREZZA IDONEE?

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

STRUMENTI SOFTWARE E HARDWARE

installati on site e gestiti internamente

SOLUZIONI IN CLOUD

CONSULENZA E SERVIZI GESTITI

Un insieme delle varie modalità

Gruppo di Lavoro
Assintel

DATA BREACH

Gruppo di Lavoro
SICUREZZA INFORMATICA
Assintel

COS'È UN DATA BREACH ?

Data Breach: è una **violazione di sicurezza** che comporta **accidentalmente o in modo illecito** la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Notifica Data Breach: la notifica della violazione di dati deve avvenire senza ingiustificato ritardo e, comunque **entro 72 ore**, dal momento in cui si è venuto a conoscenza della violazione, (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche).

Chi deve effettuare la Notifica: In caso di violazione dei dati il responsabile del trattamento, se designato, deve avvertire il titolare dell'avvenuta violazione dei dati. Quest'ultimo titolare dovrà, a quel punto, notificare l'evento all'autorità di controllo.

COME DEVE ESSERE REDATTA LA NOTIFICA DI DATA BREACH?

La notifica deve avere il **contenuto** previsto dall'art. 33 del GDPR:

Modulo di Notifica

- **Descrivere** la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- **Comunicare** il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- **Descrivere** le probabili conseguenze della violazione dei dati personali;
- **Descrivere** le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

COME COMUNICAZIONE ILDATA BREACH AGLI INTERESSATI?

Il titolare del trattamento deve **comunicare la violazione** dei dati all'interessato **senza ingiustificato ritardo** (art. 34).

Non è richiesta tale comunicazione nei seguenti casi:

- il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la **cifratura**;
- il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati
- la **comunicazione richiederebbe sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

COME GESTIRE I DATA BREACH?

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

Protocollo di Risposta	**Predisporre** policy, procedure e processi da attivare in caso di Data Breach	- Policy e Procedure di Notifica - Policy e Procedure di Comunicazione Interessati - Policy e Procedure di Incident e Crisis Management - Ecc.
Audit Periodici	**Effettuare** audit organizzativi e tecnologici per verificare la validità del Protocollo di Risposta predisposto	- Audit Organizzativo - Audit Tecnologico (Vulnerability Assessment e Network Scan)
Registro Data Breach	**Redigere** il registro dei casi di Data Breach	Registro dei Data Breach
Valutazione Data Breach	**Determinare** le modalità e le cause del Data Breach e i relativi impatti. Predisporre ed implementare le soluzioni correttive.	- Forensic Analysis - Remedian Plan - Analisi del Rischio Organizzativo e Tecnologico

Gruppo di Lavoro
SICUREZZA INFORMATICA
Assintel

IL DPO
DATA PROTECTION OFFICER

QUANDO DEVO NOMINARE IL DATA PROTECTION OFFICER?

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

OBBLIGATORIAMENTE NOMINARE UN DATA PROTECTION OFFICER (DPO)

Se la tua azienda:

- E' un organismo pubblico;
- Esercita come attività principale un trattamento che comporta la sorveglianza regolare e sistematica di soggetti su **larga scala**;
- Esercita come attività principale un trattamento di dati particolari o giudiziari su larga scala.

COME CAPIRE SE LA MIA AZIENDA RIENTRA NEI CASI DI NOMINA OBBLIGATORIA?

Attività principale (1)

Il core business di un Titolare o Responsabile del trattamento, nonché tutte le relative attività strettamente connesse.
Alcuni esempi sono: il trattamento di dati sanitari da parte di un ospedale o l'attività di sorveglianza di un certo numero di centri commerciali e spazi pubblici da parte di una società di vigilanza.

Monitoraggi o regolare e sistematico (2)

Trattamento che avviene in modo **continuo**- **ricorrente** o **costante**, secondo **modalità predeterminate- organizzate o metodiche.**
Alcuni esempi:
- programmi di fidelizzazione condotti dalla grande distribuzione;
- ogni forma di tracciamento e profilazione online anche per fini di pubblicità comportamentale;
- monitoraggio per prevenire particolari rischi (credit scoring, sistemi anti-frode e anti- riciclaggio);
- reindirizzamento di messaggi di posta elettronica;

Larga Scala (3)

Una volta individuata la pertinenza rispetto ai due criteri precedenti, per valutare un trattamento su larga scala considerare i seguenti fattori:
- la quantità di interessati coinvolti, **sia in relazione al numero che in proporzione alla popolazione pertinente**,
- il volume e il range di dati trattati,
- la durata del trattamento e l'estensione geografica.

Alcuni esempi:
- trattamento di dati relativi a pazienti svolto da un ospedale;
- trattamento di dati da parte di fornitori di servizi telefonici o telematici;
- trattamento di dati da parte di una banca di credito cooperativo di un paese con pochi abitanti.

MI CONVIENE NOMINARE IL DPO ANCHE SE NON SONO OBBLIGATO?

Valutare la nomina di un Data Protection Officer, anche in caso di facoltatività, rappresenta un importante strumento per dimostrare **ACCOUNTABILITY** e pertanto **l'**affidabilità e la competenza aziendale nella gestione dei dati personali. Tale attitudine è da incoraggiare, rappresentando altresì un plus in termini di appeal sul mercato, tenendo conto della struttura organizzativa ovvero della complessità dei trattamenti.

Gruppo di Lavoro SICUREZZA INFORMATICA Assintel

CHI NOMINO DPO?

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

DPO INTERNO

Già presente in azienda appositamente selezionato per ricoprire tale carica. Può svolgere ulteriori compiti che esulano dalla protezione dei dati, purché sia garantita l'assenza di conflitti di interesse e deve operare con un grado sufficiente di autonomia.

MA ATTENZIONE!

IL DPO E' UNA FIGURA INDIPENDENTE e riferisce direttamente ai vertici aziendali. Ciò significa che un DPO **non può rivestire**, all'interno dell'organizzazione **un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali**.

Nella pratica?
Il DPO interno potrebbe coincidere con una figura aziendale di alta professionalità, ovvero una figura interna già presente o da assumere alla quale poter anche affiancare, se necessario, un consulente esterno specializzato nel settore.

Alcuni esempi di soggetti che, per il ruolo che rivestono in azienda, **non possono essere nominati DPO**:
- Amministratore Delegato
- Direttore Finanziario
- Direttore Sanitario
- Responsabile Marketing
- Responsabile HR
- Responsabile IT

DPO ESTERNO

La funzione di DPO può essere affidata ad un soggetto esterno all'organismo o all'azienda titolare/responsabile del trattamento, sulla base di un contratto di servizi

QUALI CARATTERISTICHE DEVO CERCARE?

La funzione di DPO può essere esercitata da una **persona fisica o giuridica**.
E' indispensabile che ciascun soggetto appartenente alla persona giuridica e operante quale DPO soddisfi tutti i requisiti applicabili.

Il DPO deve avere:
- Almeno 6 anni di esperienza **in materia di data protection.**
- Approfondite conoscenze di natura Giuridica in ambito Data Protection.
- Approfondite conoscenze in ambito ICT e Cybersecurity.
- Rilevanti competenze in ambito manageriali.

Un importante riferimento, rispetto le caratteristiche professionali del DPO è la Certificazione UNI 11697:2017
Norma tecnica che definisce i requisiti relativi ai professionisti che operano nel settore della protezione dei dati personali. Un professionista dotato di certificazione UNI11697, è sicuramente dotato delle idonee conoscenze, abilità e competenze in materia.

Gruppo di Lavoro SICUREZZA INFORMATICA Assintel

COME SI DESIGNA UN DATA PROTECTION OFFICER?

L'atto di nomina è parte costitutiva dell'adempimento previsto dall'art. 37 del GDPR

DPO INTERNO

Formalizzare un apposito atto di designazione

DPO ESTERNO

L'atto di designazione costituirà parte integrante dell'apposito contratto di servizi

COME REDIGERE L'ATTO DI DESIGNAZIONE?

L'atto di designazione deve individuare i requisiti di cui agli artt. 37-38 e 39 del GDPR.
L'Autorità Garante italiana ha pubblicato sul sito ufficiale uno schema apposito, che è possibile scaricare.

DEVO COMUNICARE UFFICIALMENTE I DATI DEL DPO?

E' importante comunicare l'avvenuta designazione di un DPO alla compagine aziendale, ai soggetti interessati, individuando i canali più opportuni (ad es. In informative, sito web), ma soprattutto darne comunicazione all'Autorità Garante.

COME COMUNICO I DATI DEL DPO AL GARANTE PRIVECY?

L'Autorità ha predisposto sul sito web istituzionale una procedura informatizzata all'uopo dedicata.

COSA FA IL DPO IN AZIENDA?

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

COSA DEVE FARE IL DPO IN AZIENDA?

• **Informare e fornire consulenza** → mettere al corrente il DPO in merito a ogni iniziativa aziendale volta ad avere un risvolto sul trattamento di dati personali è fondamentale;

• **Assicurare la messa in opera degli adeguamenti**, esercitare un'azione di **controllo e vigilanza**→ il DPO definisce concretamente un piano di implementazione degli adempimenti (aggiornamento del Registro dei trattamenti, gestione della valutazione d'impatto, sorveglia il rispetto delle contromisure idonee ad assicurare la sicurezza dei dati personali);

• **Istruire i soggetti interni** all'azienda sui requisiti da rispettare per la protezione dei dati personali → il DPO diffonde la cultura in materia di protezione dei dati personali, istruisce e sorveglia la compagine in merito alla corretta gestione delle operazioni di trattamento;

• **Essere un punto di contatto per i soggetti interessati** → il DPO definisce le procedure per l'esercizio dei diritti degli interessati più idonee, prende in carico e risponde alle richieste avanzate dai soggetti.

• **Essere il punto di contatto tra l'azienda e l'Autorità Garante** →
Il DPO risponde alle richieste, si relaziona con l'Autorità in merito a controlli ed ispezioni, si occupa di notificare eventuali data breach, recuperando e fornendo le opportune informazioni richieste.

SE IL MIO DPO E' ESTERNO, QUANTE VOLTE IN UN ANNO DEVE ESSERE PRESENTE IN AZIENDA? COME FACCIO A QUANTIFICARE IL TEMPO CHE MI DEDICHERA'? COSA DEVO TENERE IN CONSIDERAZIONE?

- La complessità del trattamento di dati personali.
- La tipologia di finilità del trattamento.
- La tipologia di attività.
- La tipologia di danimicità dell'azienda.
- Il numero di sedi sia a livello nazionale che internazionale.
- La tipologia di organizzazione.
- Il tipo di supporto che viene dato dal referente interno aziendale.
- La complessità del sistema informatico.
- Il livello di sicurezza dei sistemi informativi aziendali.
- La tipologia di fornitori.
- Il livello di sensibilizzazione e formazione del personale sulla tematica.
- Il rapporto con altre legal entity dello stesso gruppo.
- Se il DPO in questione sarà «il DPO capofila» tra i DPO di un Gruppo di aziende.
- Se è un DPO di Gruppo e quindi fa il DPO per più aziende delle stesso Gruppo.

Possiamo stimare, come indicazione di massima, che un DPO, come minimo, dovrà dedicare 1 giornata uomo al mese.

QUANTO MI COSTA?

Non esiste un tariffario ufficiale, ma il tariffario viene fatto dal mercato.

Nella Pratica?

Occorre tenere in considerazione che il DPO è una risorsa altamente qualificata.
E' possible stimare come giusto compenso, un valore non inferiore ai 500 euro giorno/uomo.

Gruppo di Lavoro
SICUREZZA INFORMATICA
Assintel

Grazie per l'attenzione

Paola Generali
Managing Director
GETSOLUTION
paola.generali@getsolution.it
www.getsolution.it

Diego Perini
Senior Manager Privacy
ADFOR
diego.perini@adfor.it
www.adfor.it

Gruppo di Lavoro
SICUREZZA INFORMATICA
Assintel

@Assintel

www.assintel.it

segreteria@assintel.it