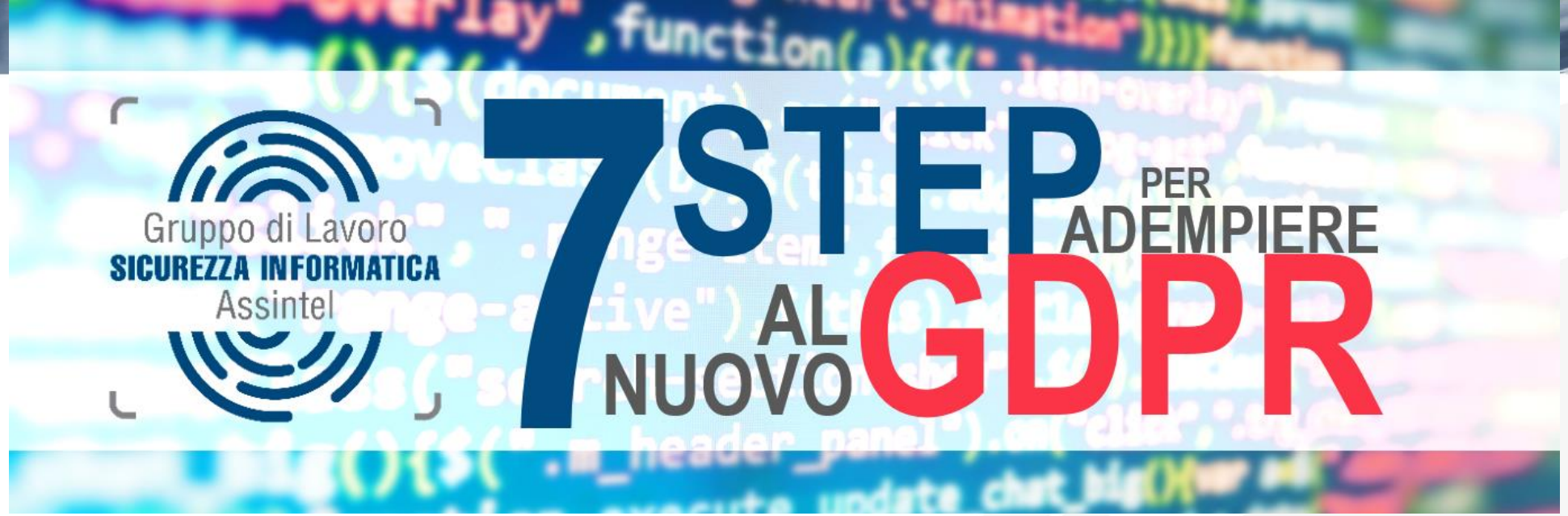


Rino Cannizzaro, *Gruppo di Lavoro Sicurezza Informatica Assintel*

Paola Generali, *Vice Presidente e Coordinatrice GdL Sicurezza Informatica di Assintel*

Il passintelligente per il tuo business

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

Il GDPR: Entrata in vigore e Recepimento

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI
(GeneralDataProtectionRegulation679/2016- GDPR)

Ha l'obiettivo di fortificare i diritti delle persone fisiche e unificare la Normativa in merito alla protezione dei dati personali all'interno di tutta l'Unione Europea, sostituendo le diverse leggi nazionali presenti nei Paesi Membri.

Il Regolamento abroga la Direttiva95/46/CE, recepita dall'attuale D.lgs. 196/2003 (c.d. Codice Privacy).

Il GDPR: Principi applicabili al trattamento (Art. 5)

Il Regolamento impone il rispetto dei seguenti Principi:

LICEITA', CORRETTEZZA E TRASPARENZA

LIMITAZIONE DELLE FINALITA':
Determinate, esplicite e legittime

MINIMIZZAZIONE DEI DATI:
Adeguati, pertinenti e limitati

ESATTEZZA:
i Dati devono essere Esatti e, se necessario, aggiornati

LIMITAZIONE DELLA CONSERVAZIONE:
Per un periodo temporale limitato al conseguimento delle finalità

INTEGRITA' E RISERVATEZZA:
Deve essere garantita un'adeguata sicurezza dei dati personali

RESPONSABILIZZAZIONE:
il Titolare è tenuto a comprovare il rispetto di tali principi

FASI DI ADEGUAMENTO AL GDPR

Saranno illustrati tutti i principali adempimenti che il GDPR introduce e ai quali le aziende dovranno assolvere. Il workshop lo farà proponendo un modello di adeguamento, fornendo **istruzioni pratiche e strumenti validi, all'interno di un percorso suddiviso in step.**

Le fasi di adeguamento proposte riguarderanno i seguenti ambiti:

1. MAPPARE DEI TRATTAMENTI;
2. INDIVIDUARE I RUOLI, LE RESPONSABILITA' E I COMPITI;
3. DEFINIRE E ATTUARE GLI ADEMPIMENTI PER PRIORITA' D'AZIONE;
4. DEFINIRE MISURE DI SICUREZZA ADEGUATE;
5. DEFINIRE POLICY E PROCEDURE ORGANIZZATIVE;
6. DEFINIRE UNA PROCEDURA DI DATA BREACH;
7. DOCUMENTARE LA CONFORMITA'

ALCUNE DEFINIZIONI FONDAMENTALI

DATI PERSONALI

Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»), direttamente o indirettamente, con un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

TRATTAMENTI

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, 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, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

STEP 1: MAPPARE I TRATTAMENTI DEI DATI PERSONALI

E’ DI FONDAMENTALE IMPORTANZA RACCOGLIERE LE INFORMAZIONI NECESSARIE PER MAPPARE LE ATTIVITÀ DI TRATTAMENTO DI DATI PERSONALI CHE L’AZIENDA SVOLGE.

Se l'azienda ha più di 250 dipendenti o svolge trattamenti che riguardano dati particolari, giudiziari o che comportano un rischio per i diritti e le libertà degli interessati

PREDISPORRE E MANTENERE AGGIORNATO UN **REGISTRO DEI TRATTAMENTI** E ASSICURARSI CHE RISPETTINO I PRINCIPI PREVISTI DAL REGOLAMENTO

Se l'azienda ha meno di 250 dipendenti e il trattamento svolto non riguarda dati particolari, giudiziari o non comporta mai un rischio per i diritti e le libertà degli interessati

VALUTARE LA PREDISPOSIZIONE DI UN REGISTRO DELLE ATTIVITÀ ANCHE SE NON OBBLIGATORIO. Ciò consente di avere una mappatura dei trattamenti utile per le altre attività di adeguamento e per dimostrare la conformità

STEP 1: IL REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

L'art. 30 del GDPR dispone che il Registro debba contenere per ogni trattamento le seguenti informazioni:

- I differenti trattamenti di Dati personali;
- Le categorie di Interessati e di dati personali trattati;
- Le finalità del Trattamento;
- I soggetti interni ed esterni coinvolti nel Trattamento di dati, tra cui l'elenco degli incaricati;
- Il flusso di Dati, in caso di trasferimento di Dati extra UE;
- Il luogo in cui i Dati sono conservati;
- Per ciascuna categoria di dati il tempo di conservazione;
- Le misure di sicurezza adottate per minimizzare i rischi.

PRIVACY BY DESIGN

Il Regolamento introduce il principio di protezione dei dati personali già **in fase di progettazione** (*byDesign*) per qualsiasi tipo di progetto che comporti l'utilizzo di dati personali (sito internet, software, soluzione IT, ambiente di lavoro, etc.).

- Pseudonimizzazione dei dati;
- Crittografia del database;
- Sistemi già predisposti alla cancellazione dei dati dopo il termine stabilito;
- Sistema integrato per la registrazione e gestione dei consensi;
- Predisposizione di informative chiare ed esaustive ;
- Adeguati processi di backup e ripristino dei dati in casi avversi;

PRIVACY BY DEFAULT

Il Regolamento impone che il titolare adotti opportune misure per garantire che siano trattati di **default solo i dati personali necessari in ogni fase del trattamento**:
dalla raccolta alla cancellazione dei dati e non soltanto durante l'elaborazione

- Minimizzazione dei dati personali già in fase di raccolta;
- Pseudonimizzazione dei dati personali;
- Periodo di conservazione dei dati limitato;
- Accesso ai dati consentito solo per soggetti autorizzati al trattamento;
- Accesso ai dati consentito per intervalli temporali brevi in caso di attività occasionali.

STEP 2: INDIVIDUARE RUOLO, RESPONSABILITA' E COMPITI

STEP 2: Titolare del Trattamento

IL **TITOLARE DEL TRATTAMENTO** È TENUTO A:

- **IMPLEMENTARE OPPORTUNE MISURE DI SICUREZZA**

Misure tecniche e organizzative

Adeguate politiche in materia di protezione dei dati

Protezione dei dati dalla progettazione e di default

Tali misure devono tener conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

- **DIMOSTRARE LA CONFORMITA'** delle operazioni di trattamento rispetto ai principi sanciti dal Regolamento, ad esempio tramite:

Registro delle categorie di attività di trattamento (per taluni casi è un obbligo)

Adesione a un meccanismo di certificazione approvato

Adesione a codici di condotta approvati

*Il Regolamento stabilisce che il soggetto interessato può richiedere al titolare il **risarcimento dei danni** subiti da un trattamento; in tal caso il titolare è tenuto a risponderne direttamente e interamente.*

STEP 2: Responsabile del trattamento

L'attribuzione di uno o più trattamenti da parte del titolare del trattamento verso un responsabile del trattamento deve essere **regolamentata tramite un contratto o altro atto giuridico**.
Gli aspetti fondamentali da definire e disciplinare sono:

L'oggetto del trattamento, la durata, la natura e la finalità	Il tipo di dati personali e le categorie di interessati	Gli obblighi e i diritti del titolare del trattamento e del responsabile del trattamento.

Come regolamentare i Subfornitori?

Il responsabile, scelto da un titolare del trattamento, **può avvalersi di un altro soggetto** solo se riceve espressa e documentata **autorizzazione dal titolare del trattamento**, il quale ha anche la facoltà di rifiutarsi.

In tal caso il responsabile è tenuto a nominare il subfornitore responsabile del trattamento e ad imporre allo stesso, tramite contratto o atto giuridico, i medesimi doveri in materia di protezione dei dati personali che il titolare gli ha prescritto.

Il responsabile del trattamento mantiene la totale responsabilità nei confronti del titolare anche nel caso in cui l'inadempienza degli obblighi in materia di protezione dei dati derivi dall'altro responsabile da lui nominato.

STEP 2: Obblighi del responsabile

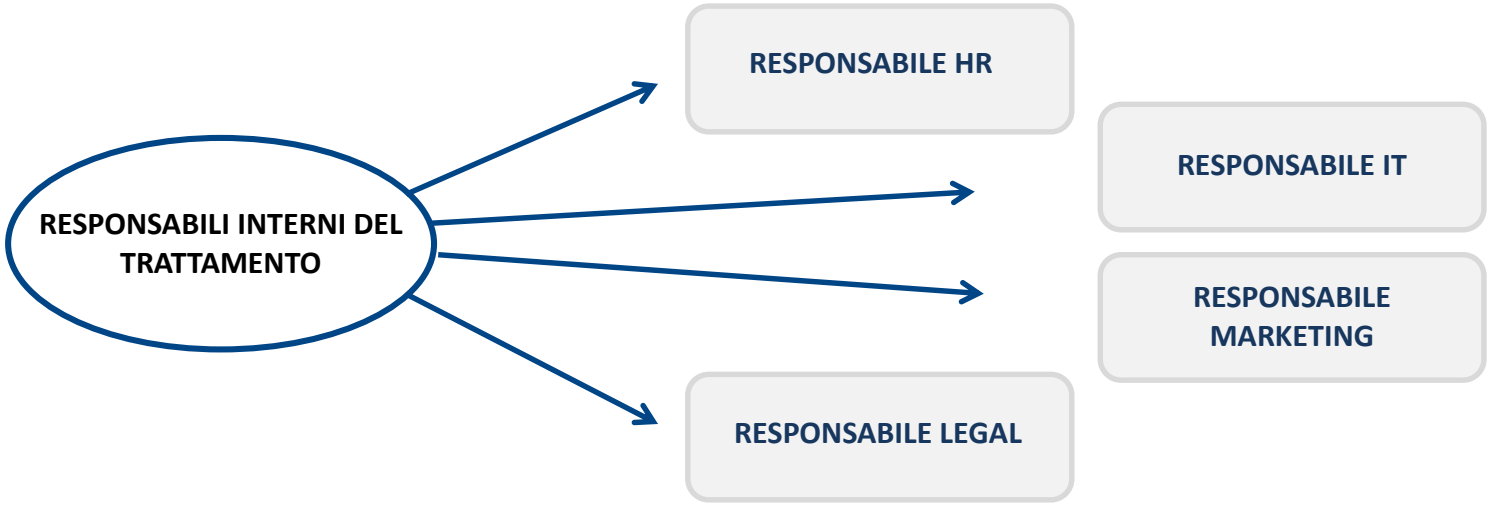
Gli obblighi in capo al **Responsabile**, da regolamentare all'interno dell'atto, sono:

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

STEP 2: Responsabile Interno del trattamento

Il Regolamento stabilisce che un soggetto che tratta dati personali per conto di un Titolare agisce in qualità di Responsabile.

Il Titolare potrà nominare soggetti interni Responsabili del trattamento, tuttavia su di essi non potranno ricadere i medesimi compiti previsti dal Regolamento per i Responsabili Esterni.



STEP 2: Soggetti autorizzati al trattamento

Qualsiasi persona che agisce sotto l'autorità del Titolare del trattamento o Responsabile, che ha accesso ai Dati personali, **può trattarli solo su istruzione del Titolare** o se è imposto dalla legge o degli Stati Membri dell'Unione.

INCARICATO DEL TRATTAMENTO

Soggetto che ha accesso ai Dati personali e li elabora sotto l'autorità del Titolare del trattamento o Responsabile.

STEP 2: Il Contitolare

Il Regolamento introduce il principio di "**Contitolarità**" quando due o più soggetti possono svolgere dei trattamenti congiunti.

I Contitolari devono stabilire mediante un accordo interno:

- ✓ le rispettive responsabilità in relazione agli obblighi in materia di protezione dei dati;
- ✓ il soggetto che sarà individuato come punto di contatto unico per l'esercizio dei diritti degli interessati;
- ✓ le modalità per l'espletamento delle richieste di diritto d'accesso ai dati;
- ✓ le modalità per fornire un'adeguata informativa agli interessati;
- ✓ i rispettivi ed effettivi ruoli dei contitolari, soprattutto nei confronti degli interessati.

Il contenuto essenziale dell'accordo deve essere reso disponibile agli Interessati.

STEP 2: IL DATA PROTECTION OFFICER

Individuare i Ruoli, Responsabilità, Compiti

Ai fini della gestione dei Dati Personali raccolti presso l'azienda il GDPR ha previsto l'individuazione di un vero "direttore d'orchestra" che eserciti una funzione di informazione, consiglio e controllo interno:

Il DATA PROTECTION OFFICER (DPO)

STEP 2: IL DPO

Il DPO è il soggetto a cui il Titolare, o il Responsabile, si affida per **garantire la conformità dell'organizzazione ai requisiti stabiliti dal Regolamento**. Il DPO agisce in modo indipendente e riferisce direttamente ai vertici.

E' designato in funzione delle **qualità professionali**, in particolare della conoscenza specialistica della normativa e delle prassi in **materia di protezione dei dati**, e della capacità di assolvere i compiti di cui all'arti. 39 GDPR

STEP 2: IL DPO

Se l'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.

OBBLIGATORIAMENTE NOMINARE UN DATA PROTECTION OFFICER (DPO)

STEP 2: IL DPO

SE L'AZIENDA NON RIENTRA FORMALMENTE NELL'OBBLIGO DI NOMINARE UN DATA PROTECTION OFFICER

Individuare uno o più soggetti (esterni e/o interni all'organizzazione)che si occupino degli adeguamenti al Regolamento

Valutare l'opportunità di nominare comunque un DPO

STEP 2: COMPITI E RESPONSABILITA' (Art. 39)

- Informare e consigliare il titolare sugli obblighi concernenti il Regolamento;
- Assicurare la messa in opera degli adeguamenti;
- Istruire i soggetti interni all'azienda sui requisiti da rispettare per la protezione dei dati personali;
- Sorvegliare il rispetto del regolamento;
- Dialogare con le autorità competenti e i soggetti interessati ove necessario;
- Comprendere i rischi connessi al trattamento di dati personali e suggerire le misure per contenerli.

RESPONSABILITA'

Il controllo del rispetto del regolamento non significa che il DPO sia **personalmente responsabile** in caso di inosservanza. Il GDPR chiarisce che il rispetto delle norme in materia di protezione dei dati fa parte della **responsabilità d'impresa del titolare del trattamento, non del DPO**.

In caso di inadempimenti derivanti da colpa o dolo del DPO, il Titolare o il Responsabile potrà avanzare pretese risarcitorie a titolo di responsabilità contrattuale.

STEP 2: Posizione del DPO

Al DPO è consentito di "**svolgere altri compiti e funzioni**", ma a condizione che il titolare o il responsabile del trattamento si assicuri che "tali compiti e funzioni **non diano adito a un conflitto di interessi**".

L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza.
Ciò significa, in modo particolare, che un DPO **non può rivestire**, all'interno dell'organizzazione del titolare o del responsabile, **un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali**.

Per tale motivazione, **le Linee Guida** forniscono 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

STEP 2: Tipologie di DPO

Soggetto Interno	Soggetto Esterno	Persona Fisica o Giuridica	Team	Condiviso
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.	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**	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**: per esempio, è indispensabile che nessuno di tali soggetti versi in situazioni di conflitto di interessi.	Per favorire una corretta e trasparente organizzazione interna e prevenire conflitti di interesse a carico dei componenti si raccomanda di procedere a una **chiara ripartizione dei compiti all'interno del team DPO** e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun Titolare.	Può essere designato da associazioni e altri organismi di categoria **solamente nei casi in cui NON rientri nell'obbligo di nomina**, tenuto conto della struttura organizzativa e delle dimensioni. **Assicura supporto alle aziende** che decidono di usufruire della sua funzione e di aderire al relativo Codice di Condotta

Definire e attuare gli adempimenti necessari per priorità d'azione

Dopo aver mappato i trattamenti, è necessario identificare per ciascuno di questi le attività da effettuare per essere conformi al Regolamento.

Gli adeguamenti dovranno essere categorizzati per priorità in base ai rischi per i diritti e le libertà dei soggetti.

STEP 3: DEFINIRE E ATTUARE GLI ADEMPIMENTI PER PRIORITA' D'AZIONE

Le principali attività saranno:

- Assicurarsi che siano trattati solo i dati personali strettamente necessari alle finalità di trattamento;
- Identificare la base giuridica del trattamento (consenso, interesse legittimo, contratto, obblighi legali);
- Revisionare tutte le informative per essere conformi al Regolamento;
- Regolamentare i rapporti con i Responsabili del trattamento;
- Verificare che gli incaricati del trattamento siano a conoscenza degli obblighi in materia di protezione dei dati personali e che siano presenti clausole di riservatezza;
- Prevedere le modalità d'esercizio dei diritti degli interessati;
- Valutare e adottare le misure di sicurezza adeguate .

STEP 3: DEFINIRE E ATTUARE GLI ADEMPIMENTI PER PRIORITA'D'AZIONE

Se l'azienda:

- Tratta dati particolari o giudiziari;
- Effettua attività di sorveglianza sistematica di un'area accessibile al pubblico;
- Svolge attività di valutazione sistematica di aspetti personali dei soggetti, tra cui la profilazione;
- Trasferisce dati personali fuori dall'UE.

Ulteriori adempimenti:

- **Valutazione di impatto per la protezione dei dati personali (PIA);**
- **Informative specifiche e dettagliate;**
- **Raccolta di consensi specifici;**
- **Garanzie per il trasferimento dei dati Extra UE;**
- **Determinazione delle misure di sicurezza adeguate da mettere in atto in considerazione dei rischi.**

Definizione delle Misure di sicurezza Adeguate
Gestire i rischi

Se sono stati individuati trattamenti di Dati Personali suscettibili di generare dei rischi elevati per i diritti e le libertà dei Soggetti Interessati, dovrà essere eseguita, per ognuno dei trattamenti, un’analisi d’impatto sulla protezione dei dati

STEP 4: GESTIRE I RISCHI

Ogni Titolare del Trattamento dovrà determinare le **misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio e al trattamento**

Se l'azienda ha identificato dei trattamenti di dati personali che possano comportare dei **rischi per i diritti e le libertà dei soggetti interessati**

Condurre una Valutazione d'impatto per ciascun trattamento di dati personali a rischio

STEP 4: DATA PROTECTION IMPACT ASSESSMENT (DPIA)

La DPIA è una procedura che ha lo scopo di **Costruire e Dimostrare la Compliance** ai requisiti del Regolamento 679/2016.
Importante **strumento di Accountability** si realizza attraverso:

La **valutazione delle attività** di cui si compone il trattamento dei dati personali alla luce dei principi di necessità e proporzionalità;

La **gestione dei rischi** nei confronti dei diritti e libertà individuali derivanti dal trattamento dei dati personali.

Eseguire una DPIA non è obbligatorio per ogni operazione, ma soltanto quando il trattamento dei dati ha **un'alta probabilità di rischi nei confronti dei diritti e libertà individuali** derivanti dal trattamento dei dati personali, **sebbene in termini di buona prassi costituisca un modo per il Titolare/Responsabile di dimostrare responsabilità e trasparenza** attraverso la predisposizione di misure di sicurezza adeguate al contesto e al rischio.

STEP 4: ALTA PROBABILITA'DIRISCHIO:I CRITERI DA CONSIDERARE(DPIA)

Decisioni automatiche che producono sui soggetti interessati degli effetti legali o simili. Per esempio una decisione potrebbe produrre degli effetti discriminatori o di esclusione nei confronti di individui

Valutazioni o Registrazioni
Inclusa profilazione, di aspetti che riguardano le performance lavorative, la salute, le condizioni economiche, gli interessi personali ecc…

Controllo sistematico
utilizzato per osservare e controllare i soggetti interessati

Trasferimento dei Dati al di fuori dell'Unione Europea

Dati trattati su larga scala

Usi innovativi e applicazione di soluzioni tecnologiche.
E' necessaria una DPIA in quanto dalle nuove tecnologie possono generarsi forme nuove di raccolta dati e utilizzo di dati

Dati che riguardano "Soggetti Vulnerabili"
è necessaria una DPIA a causa dello squilibrio tra le posizioni del Data Controller e dei soggetti interessati

Set di Dati
originati per esempio dalla combinazione di due o più operazioni nel trattamento di Dati con finalità diverse o ad opera di differenti Titolari e/o Responsabili

Quando **il trattamento in sé non consente ai soggetti interessati di esercitare un diritto** o utilizzare un servizio o un contratto

Dati sensibili

STEP 4: MISURE TECNICHE E ORGANIZZATIVE

Il Regolamento introduce l'obbligo di attuare misure di sicurezza **ADEGUATE** in considerazione dei seguenti elementi:

Lo stato dell'arte e i costi di attuazione

La natura e il campo di applicazione del trattamento

Il contesto e le finalità del trattamento

Il rischio, la probabilità e la gravità delle conseguenze per i diritti e le libertà delle persone.

STEP 4: MISURE TECNICHE E ORGANIZZATIVE

Il Regolamento stabilisce che la sicurezza dei dati deve basarsi sui seguenti aspetti fondamentali:

MISURA TECNICA →

- **Pseudonimizzazione o crittografia dei dati;**

REQUISITI DI SICUREZZA →

- **Garanzie di riservatezza, integrità, disponibilità e recupero dei dati personali e dei sistemi che li custodiscono e li elaborano;**
- **Accesso tempestivo ai dati in caso di un evento dannoso fisico o tecnico;**
- **Processi di verifica periodica dell'efficacia ed effettiva applicazione delle misure di sicurezza in atto.**

STEP 5

Definizione di Policy e Procedure
Procedure Organizzative Interne

Per garantire un alto livello di protezione dei Dati Personali porre in essere delle Procedure Interne che garantiscano la protezione dei Dati in tutti i momenti, tenendo in considerazione gli eventi che possono sopravvenire nel corso del Trattamento.

STEP 5: PROCEDURE ORGANIZZATIVE INTERNE

Per **garantire un adeguato livello di protezione dei dati personali**, implementare procedure interne organizzative che tengano in considerazione qualsiasi evento che possa avere un impatto sul trattamento di dati personali nel caso si verifichi (vulnerabilità, incidenti, violazione dei dati, esercizio dei diritti, etc.)

Procedure interne che comprendano:

- Il rispetto del principio della protezione dei dati già in fase di progettazione di un'applicazione o di un trattamento e di default;
- La formazione e la sensibilizzazione dei soggetti interni che trattano dati personali;
- La gestione dei reclami e delle richieste di esercizio dei diritti da parte degli interessati;
- La prevenzione e la gestione di violazioni ai dati personali, tra cui l'obbligo di notifica all'autorità Garante ed eventualmente agli interessati.

Procedura di Data Breach

Attuare misure tecniche, organizzative e procedurali al fine di individuare e gestire tempestivamente una violazione dei dati personali e la relativa notifica

STEP 6: DATA BREACH

Nel caso in cui si verifichi una violazione dei dati personali che possa in qualche modo tradursi in un rischio per i diritti e le libertà degli individui, qualsiasi **titolare del trattamento** ha l'obbligo normativo di notificare l'avvenimento all'Autorità di controllo.

Il titolare del trattamento è tenuto ad **informare gli interessati** tempestivamente se la violazione può comportare una **grave ed elevata compromissione dei loro diritti e delle libertà**, come nel caso di:

Danni fisici, materiali o morali	**Limitazione dei diritti**	**Discriminazione**	**Furto o usurpazione d'identità**	**Perdita del controllo dei dati**

Non è necessaria la comunicazione ai soggetti interessati se il titolare del trattamento ha applicato le **opportune misure tecnologiche e organizzative preventive**(esempio crittografia dei dati) o è stato in grado di **evitare tempestivamente il verificarsi di rischi elevati**.

STEP 6: DATA BREACH

Elementi essenziali da riportare all'interno della Notifica di violazione all'Autorità:

- La natura della violazione dei dati personali e le circostanze in cui si è verificata;
- Il numero approssimativo di soggetti interessati coinvolti ;
- Le categorie e il numero approssimativo di registrazioni dei dati oggetto della violazione;
- I riferimenti del responsabile della protezione dei dati o di un altro punto di contatto;
- Le probabili conseguenze della violazione dei dati personali;
- Le misure già adottate o che il titolare intende adottare per ridurre le conseguenza e porre rimedio alla violazione dei dati personali.

STEP 6: DATA BREACH

Contromisure necessarie per la **gestione di una violazione** e per limitarne gli effetti:

Misure tecniche che riconoscano all'istante la violazione e allertino prontamente il titolare o il responsabile;

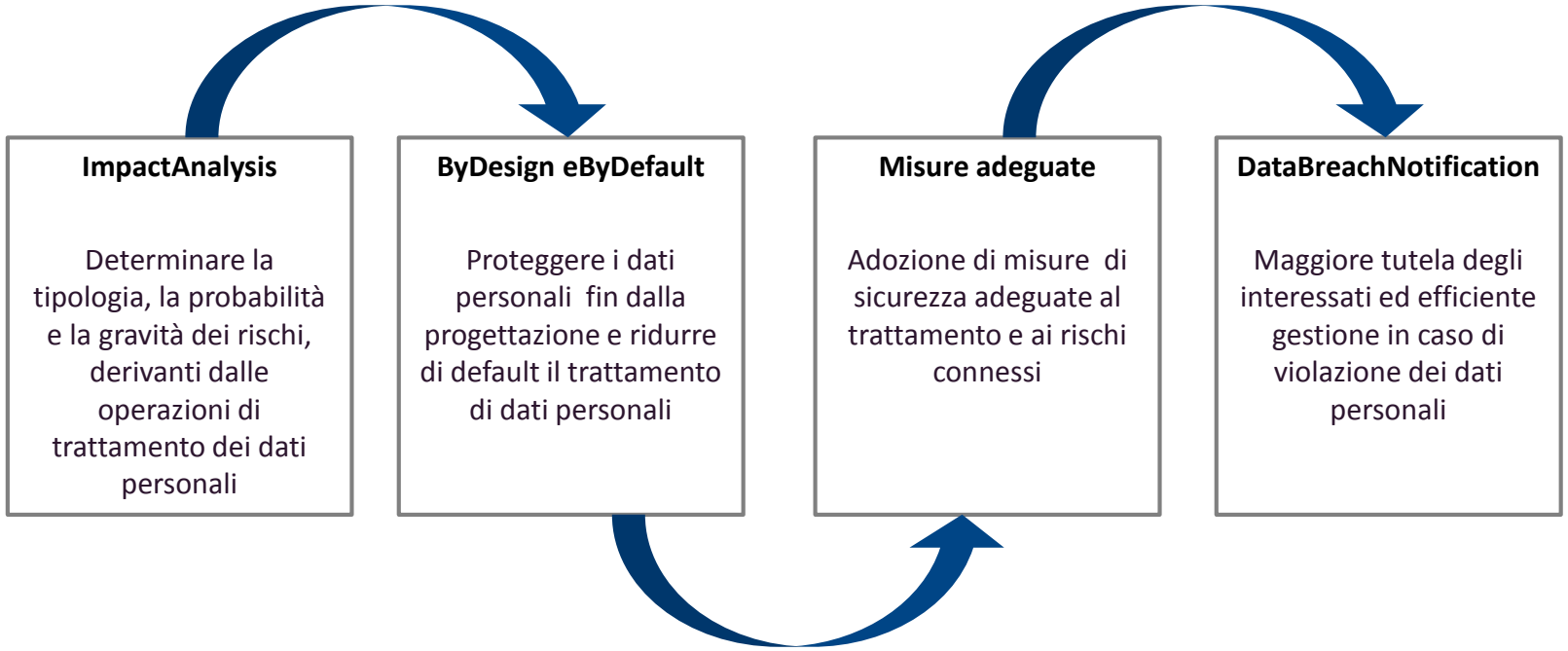
Sensibilizzazione dei responsabili del trattamento e dei soggetti autorizzati al trattamento, anche tramite adeguate policy, affinché si possa agire correttamente e tempestivamente in caso di databreach;

Mezzi adeguati per l'invio della comunicazione ai soggetti interessati quando dovuto, tenendo in considerazione che la violazione potrebbe anche compromettere i dati presenti a sistema;

Misure atte a rendere non intellegibili e criptati i dati oggetto di violazione per chiunque non sia autorizzato ad accedervi;

STEP 6: ADEGUATO LIVELLO DI PROTEZIONE

DALL'IMPACT ANALYSIS AL DATA BREACH



Documentare la conformità

Per dimostrare di essere conformi al GDPR è necessario raccogliere la documentazione necessaria. Le attività e i documenti posti in essere in ogni fase del Trattamento dovranno essere riesaminati e aggiornati regolarmente per assicurare una protezione dei Dati permanente

STEP 7: DOCUMENTARE LA CONFORMITA’

Per provare la conformità al Regolamento, predisporre e tenere aggiornata la documentazione necessaria.

- Documentazione attestante i trattamenti di dati personali svolti (Registro delle attività di trattamento, valutazione d'impatto, la documentazione prevista per il trasferimento dei dati Extra UE);
- Documentazione attestante il rispetto dei diritti e delle libertà dei soggetti interessati (le informative, i moduli di raccolta consensi, l'attestazione dei consensi raccolti, la gestione dei diritti esercitati);
- Documentazione che definisce i ruoli e le responsabilità in materia di protezione dei dati personali (i contratti e le nomine dei responsabili esterni, la gestione degli incaricati del trattamento, le procedure interne, etc.);
- Comprova delle misure di sicurezza tecniche implementate (analisi dei log, report, configurazioni, policy, etc.).

Grazie per l'attenzione

Dott. Rino Cannizzaro
Amministratore Delegato
ADFOR
rino.cannizzaro@adfor.it
cell: 335-5872913
www.adfor.it

Dott.ssa Paola Generali
Managing Director
GETSOLUTION
paola.generali@getsolution.it
cell: 335-5366986
www.getsolution.it

@Assintel

GdLAssintel SicurezzaInformatica