Fastweb Digital Academy

PROTEGGERE I DATI PERSONALI E LA PRIVACY

Avv. Matteo Pedica
Data Protection Officer

DAI PRINCIPI DEL GDPR...

ACCOUNTABILITY

TRASPARENZA

MINIMIZZAZIONE

INTEGRITA' E RISERVATEZZA

LIMITAZIONE DELLE FINALITA' DEI TRATTAMENTI

ESATTEZZA

LICEITA' E CORRETTEZZA

LIMITAZIONE DELLA CONSERVAZIONE

PRIVACY BY DESIGN & DEFAULT

F D A
Fastweb Digital Academy

...ALL'ACCOUNTABILITY IN CONCRETO

E' il **pilastro** della conformità al **GDPR.**

Si sostanzia nell'**assunzione del rischio** derivante dal trattamento di dati.

Chi tratta dati deve valutare in autonomia i rischi e gestirli di conseguenza.

In concreto si traduce nell'adozione di comportamenti e misure tecniche adeguati a garantire – e **dimostrare**- l'applicazione del regolamento ai trattamenti di dati personali

Misure tecniche

Misure organizzative
- Policy interne
- Formazione

Documenti a comprova

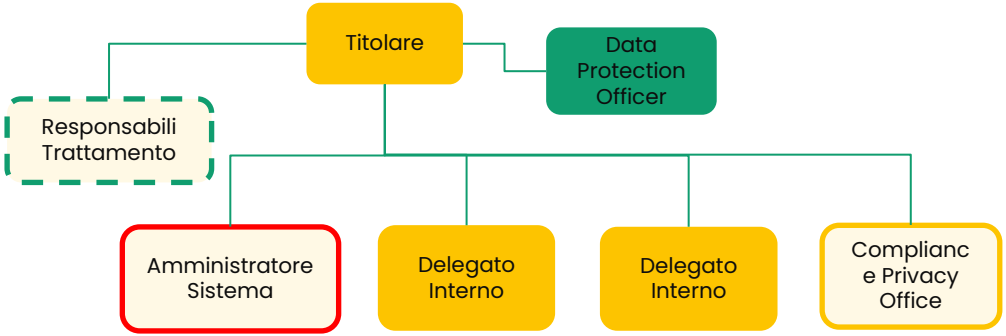
Fastweb Digital Academy

GLI ADEMPIMENTI

Policy gestione Dati Personali	Adottare Privacy by Design & Default	Compilare Registro Trattamenti	Garantire Diritti Interessati
Redigere Informative Privacy	Valutare Rischi e fare DPIA	Gestire e notificare Data Breach	Nominare Responsabili del trattamento
Nominare DPO	Designare Incaricati e Amministratori di Sistema	Formare	Continuous Monitoring

POLICY

Prioritario **definire** internamente ruoli e responsabilità.



Adottare un regolamento che definisca **regole** di comportamento da seguire per approcciare in maniera corretta al trattamento dati.

Prevedere politiche di **Data Retention** e **Minimizzazione**.

PRIVACY BY DESIGN & DEFAULT

Manifestazione diretta dell'**accountability**.

Garantire che i trattamenti siano conformi ai principi del **GDPR**.

Adottare processi e procedure che esaminano il trattamento fin dall'origine e, già in fase di progettazione, adottare le opportune misure di sicurezza, tecniche e organizzative.

Ideazione

Analisi
Risk Based

Adozione
misure

Avvio
trattamento

REGISTRO DEI TRATTAMENTI

Censire i trattamenti di dati personali eseguiti dall'amministrazione.

Mapparli, prendendo in considerazione sistemi e soggetti coinvolti.

Tenerne traccia in un documento organizzato.

Aggiornarli.

Le informazioni essenziali:

- dati del titolare del trattamento;
- finalità del trattamento;
- categorie di interessati e di dati personali;
- termini per la cancellazione dei dati;
- destinatari a cui i dati personali sono stati o saranno comunicati;
- trasferimenti verso un paese terzo o un'organizzazione internazionale;
- descrizione misure di sicurezza;

I DIRITTI ESERCITABILI SUI DATI PERSONALI

Diritto di Accesso

L'Interessato ha il diritto di sapere se sia in corso il trattamento dii suoi dati personali e chiederne una copia.

Diritto di Rettifica

L'interessato ha il diritto di ottenere la modifica dei relativi dati personali inesatti o obsoleti.

Diritto di Limitazione del trattamento

L'interessato ha il diritto di negare il trattamento dei dati futuro.

Diritto di Opposizione

L'interessato ha il diritto di opporsi in qualsiasi momento al trattamento di suoi dati.

Diritto alla Portabilità

L'interessato ha il diritto di ricevere i dati personali che lo riguardano e che lui stesso ha fornito e ha il diritto di trasmettere tali dati a un altra entità.

Diritto di Cancellazione

L'interessato ha il diritto di chiedere la cancellazione dei propri dati se i dati personali.

F D A
Fastweb Digital Academy

INFORMATIVA PRIVACY 1/2

E’ una dichiarazione con cui il Titolare illustra come intende raccogliere, gestire, conservare ed elaborare i dati.

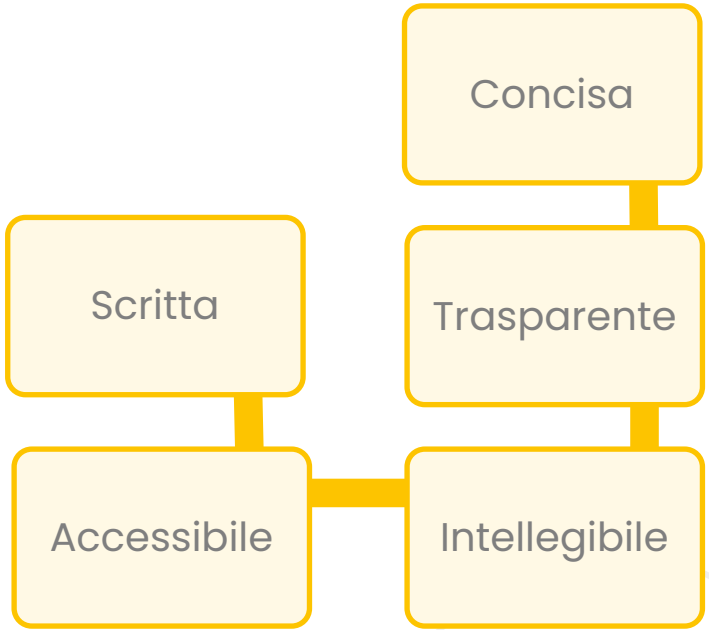
Indica anche se i dati sono mantenuti riservati o se condivisi o venduti a terzi.

Deve essere fornita all’interessato tendenzialmente prima dell’inizio del trattamento dei dati personali, quindi prima ancora che diventi interessato.

Necessaria un’informativa distinta per ogni trattamento e tipo di interessato.

INFORMATIVA PRIVACY 2/2

- Chi è il titolare dei dati e il suo indirizzo;
- Dati del DPO;
- Come e perché i dati verranno trattati;
- Base giuridica;
- Quali dati personali saranno trattati;
- Presenza di operazioni automatizzate;
- I dati vengono trasferiti a soggetti terzi;
- I dati vengono trasferiti in Paesi Terzi fuori dall'UE;
- Tempi di conservazione;
- Come esercitare i diritti dell'interessato;



VALUTARE RISCHI

Il **GDPR** sposa un approccio **Risk Based** al trattamento di dati personali.

Viene affidato ai titolari il compito di identificare i rischi e decidere **autonomamente** le modalità, le garanzie e i limiti del trattamento dei dati personali.

Il rischio inerente al trattamento è quello di impatti negativi sulle libertà e i diritti degli interessati

Gli impatti dei trattamenti vanno analizzati tramite un processo di valutazione* che consideri i rischi noti o possibili e delle misure tecniche e organizzative che il titolare potrebbe adottare per mitigare tali rischi.

Il titolare decide in autonomia se **iniziare o meno** il trattamento

*Tool per valutazione rischi di ENISA https://www.enisa.europa.eu/news/enisa-news/securing-personal-data-a-risky-business

DPIA 1/2

E’ una procedura prevista dal GDPR per **valutare** non solo la **necessità** e **proporzionalità** di un trattamento, ma anche per identificare i rischi ed **approntare misure** di scurezza idonee.

Va condotta prima di iniziare un trattamento.

Deve essere eseguita dal Titolare in consultazione con il DPO

DPIA 2/2

Eseguire la DPIA è obbligatoria quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche:

- trattamenti valutativi o di scoring, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici;
- monitoraggio sistematico;
- trattamento di dati sensibili, giudiziari;
- trattamenti di dati personali su larga scala;
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche;
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto;

DATA BREACH 1/3

Il **GDPR** non si occupa direttamente della gestione degli eventi che costituiscono **incident**

Alcune norme -*Perimetro Sicurezza DPCM 131/2020 e NIS DL 65/2018*- disciplinano **l'incident** e lo definiscono come:

«*ogni evento di natura accidentale o intenzionale -esterno o interno all'organizzazione- che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici*»

Quindi è **incident** l'evento fuori delle operazioni standard che causa, o potrebbe causare, un interruzione o una riduzione della qualità' del servizio.

DATA BREACH 2/3

Il **GDPR** presuppone che il titolare adotti metodologie atte a prevenire rischi e minacce idonee a causare una perdita di riservatezza, integrità e disponibilità dei dati personali.

Si verifica un **incident** di sicurezza;

Dalle analisi emerge che l'**incident** ha compromesso -o potrebbe compromettere- uno dei tre principi «confidenzialità/riservatezza», «integrità» e «disponibilità» della sicurezza delle informazioni:

- violazione della confidenzialità/riservatezza: divulgazione dei dati o accesso agli stessi non autorizzati o accidentali;
- violazione dell'integrità: modifica non autorizzata o accidentale dei dati;
- violazione della disponibilità: perdita o distruzione non autorizzate o accidentali di dati;

Tra le informazioni di cui l'**incident** ha leso -o potrebbe ledere- la sicurezza, sono presenti dati personali:

- Dato personale: qualsiasi informazione che consenta, direttamente o indirettamente, di identificare una persona fisica e può fornire informazioni sulle sue caratteristiche, abitudini, stile di vita, relazioni, stato di salute,;
- L'identificazione richiede elementi che permettono di distinguere una persona dalle altre;

DATA BREACH 3/3

Entro 72 ore da quando si verifica l' **incident** occorre :

- comprendere natura della violazione;
- comprendere causa della violazione;
- Identificare categorie di dati personali oggetto di violazione;
- descrivere i sistemi e le infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione;
- descrivere le misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti;
- descrivere le misure tecniche e organizzative adottate (o di cui si propone l'adozione20) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati;

Trasmettere un **incident** Report al DPO per la notifica all'autorità **entro 72 ore** da quando si verifica l' **incident**;

DATA PROTECTION OFFICER 1/2

- La nomina del DPO è un **obbligo** per le Pubbliche Amministrazioni;
- Il DPO deve essere autonomo ed **indipendente**;
- Va designato in funzione delle qualità professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati;
- È figura apicale;
- Può essere un dipendente del Titolare oppure un consulente esterno che assolve i suoi compiti in base a un contratto di servizi;
- I suoi dati vanno comunicati al Garante per la protezione dei dati personali e resi pubblici;

DATA PROTECTION OFFICER 2/2

- E’ preferibile che il DPO interno sia un dirigente o un funzionario di alta professionalità;
- I DPO **non rispondono personalmente** in caso di inosservanza del GDPR;
- Deve avere le **risorse necessarie** e il potere di spesa per assolvere ai compiti assegnati, accedere ai dati personali e ai trattamenti e per mantenere le proprie conoscenze specialistiche;

LA PARANOIA È UNA VIRTÙ

FATEVI DOMANDE

CONDIVIDETE LE INFORMAZIONI

SE AVETE DUBBI CHIAMATE IL DPO

Fastweb Digital Academy

GRAZIE