Progettato e realizzato da

Commissionato da

CORSO GDPR - Regolamento UE 2016/679 - e sicurezza informatica

commissionato da Università degli Studi di Torino

realizzato e progettato da CSI Piemonte

Modulo 1 – Persone e ruoli

Sommario

Obiettivi

In questa prima sezione dedicata alle novità del GDPR – ambito di intervento **Persone e Ruoli** – analizziamo le seguenti tematiche:

- ✓ **Tipologia di dati**
- ✓ **I soggetti**
- ✓ **I diritti degli interessati**
- ✓ **Ambito territoriale**
- ✓ **Formazione**

Torna al sommario

Tipologia di dati: i dati sensibili e giudiziari

Categorie particolari di dati

Quelli che erano i dati «sensibili» sono diventati **«particolari»** (dati sanitari, dati che rivelano l'origine razziale o etnica, l'orientamento politico, sindacale, religioso o filosofico).

Sono stati aggiunti in forma esplicita: i dati genetici e quelli biometrici.

Dati relativi a condanne penali e reati

Sono sostanzialmente i **dati «giudiziari»** previsti nel codice privacy.

Torna al sommario

GDPR: i soggetti

Il GDPR prevede, per il **trattamento dati, nuovi ruoli** che si aggiungono a quelli già esistenti.

Vediamoli nel dettaglio:

Il Titolare

Definisce finalità e mezzi del trattamento.

È il soggetto che, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è conforme al GDPR:

- ✓ deve valutare attentamente le situazioni di contitolarità e regolamentarle con accordi interni
- ✓ se affida ad un altro soggetto alcune attività, deve nominarlo Responsabile del trattamento e definire molto dettagliatamente i compiti che gli assegna
- ✓ può aderire ai Codici di condotta o agli schemi di certificazione (quando verranno istituiti) per dimostrare di essere conforme al GDPR

Il Responsabile

Mette in atto – per conto del Titolare - misure tecniche ed organizzative *adeguate* per garantire ed essere in grado di dimostrare che il trattamento è conforme al GDPR

- ✓ deve essere scelto unicamente fra soggetti che presentano garanzie sufficienti per dimostrare di essere in grado di mettere in atto misure adeguate
- ✓ può nominare dei sub-responsabili per l'esecuzione di specifiche attività (previa autorizzazione del Titolare)
- ✓ supporta il Titolare nel garantire il rispetto dell'obbligo di: dar seguito alle richieste per l'esercizio dei diritti dell'interessato, notifica delle violazioni all'Autorità di Controllo (data breach), comunicazione delle violazioni all'interessato, valutazione di impatto sulla protezione dei dati e consultazione preventiva

- ✓ essendo prevista una responsabilità in solido con il Titolare, non risponderà del danno cagionato ad un interessato soltanto se è in grado di dimostrare di aver rispettato le prescrizioni del GDPR e le istruzioni date dal Titolare
- ✓ se determina finalità e mezzi di un trattamento è considerato a tutti gli effetti Titolare del trattamento

DPO

Il Titolare e il Responsabile devono nominare un DPO quando il trattamento:

- ✓ è svolto da un soggetto pubblico
- ✓ Richiede, per la sua natura, finalità o ambito di applicazione, il monitoraggio regolare e sistematico di interessati su larga scala (es. videosorveglianza di locali aperti al pubblico)
- ✓ Riguarda dati particolari o giudiziari, su larga scala (es. il trattamento dei dati particolari da parte di un ospedale)

È il soggetto che:

- ✓ Deve essere tempestivamente coinvolto in tutte le questioni riguardanti la protezione dei dati
- ✓ Deve avere autonomia, anche economica, e riferisce direttamente al vertice gerarchico
- ✓ Può essere interno o esterno, può assumere altri compiti che però non devono dare adito a situazioni di conflitto di interessi

Nota: il gruppo di lavoro dell'Autorità Garante Europea - Working Party art. 29 - hanno individuato come possibili situazioni di conflitto di interesse, l'Amministratore Delegato, il Direttore Marketing, il Direttore Risorse Umane, il Direttore IT

Compiti del DPO:

- ✓ Informare e fornire consulenza al Titolare o al Responsabile in merito agli obblighi derivanti dal GDPR
- ✓ Sorvegliare l'osservanza del GDPR
- ✓ Sensibilizzare e formare il personale
- ✓ Se richiesto, fornire pareri su DPIA e sorvegliarne lo svolgimento
- ✓ Fungere da punto di contatto per l'Autorità di Controllo e per gli interessati

Contitolari

due o più titolari del trattamento possono determinare congiuntamente le finalità e i mezzi del trattamento e devono definire in un accordo interno i rispettivi ruoli e responsabilità.

Sub-responsabili

Il Responsabile del trattamento può ricorrere ad altro responsabile con l'autorizzazione scritta del titolare per l'esecuzione di specifiche attività di trattamento dati.

Incaricato

tale figura non è presente nel Regolamento Europeo il quale individua le persone autorizzate a compiere operazioni di trattamento sotto l'autorità del titolare o del responsabile del trattamento.

Garante (autorità di controllo)

Ogni Stato dell'Unione europea ha la sua Autorità di controllo, che è competente per la **gestione dei reclami** ad essa proposti o di **eventuali violazioni del regolamento** europeo e delle norme nazionali in materia di protezione dei dati.

Ha il potere di irrogare sanzioni, conoscere direttamente delle controversie in materia di dati personali e di effettuare controlli.

Ogni persona, in qualità di **Interessato**, può **tutelare i propri dati personali** esercitando i diritti che il GDPR amplia in modo sostanziale.

Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibili fino a 3 mesi in casi di particolare complessità.
Vediamo quali sono i diritti dell'Interessato.

Torna al sommario

I diritti dell'interessato

DIRITTO DI ACCESSO

Consiste nel **diritto di avere una copia dei propri dati.** Il Titolare (con la collaborazione del Responsabile) deve fornire un riscontro scritto entro 1 mese (orale solo se richiesto). Può essere consentito un accesso da *remoto.*

DIRITTO DI OPPOSIZIONE

L'interessato può avvalersi del diritto di **opposizione** per motivi connessi alla sua situazione particolare.
Ad esempio: il soggetto che si oppone al trattamento dei suoi dati da parte di un operatore telefonico per finalità di marketing.

DIRITTO DI RETTIFICA DEI DATI INESATTI

Il GDPR riconosce all'interessato il diritto di richiedere la **rettifica dei dati inesatti.**

DIRITTO ALL'OBLIO

L'interessato può avvalersi del diritto **alla cancellazione (oblio)** senza ingiustificato ritardo dei propri dati se: i dati non sono più necessari rispetto alla finalità dichiarata, l'interessato revoca il consenso o si oppone al trattamento, i dati sono trattati illecitamente.

DIRITTO ALLA PORTABILITA' DEI DATI

Il diritto alla portabilità dei dati consiste **nel diritto di ricevere in un formato strutturato, d'uso comune e leggibile da dispositivo automatico**, i dati che riguardano l'interessato nei casi in cui il trattamento si basa sul consenso dato o su un contratto fra le parti.

NO AL TRATTAMENTO AUTOMATIZZATO

L'interessato ha il diritto di **non** essere sottoposto a una decisione basata unicamente sul **trattamento automatizzato**, compresa la **profilazione**, che produca effetti giuridici che lo riguardano.

DIRITTO DI LIMITAZIONE AL TRATTAMENTO

L'interessato ha il diritto di ottenere la **limitazione del trattamento** quando contesta l'esattezza dei dati, quando il trattamento è illecito, o quando ha esercitato anche il diritto di opposizione.

Ad esempio: il soggetto che chiede che i suoi dati non siano temporaneamente pubblicati su un sito web.

Tutti i diritti possono essere «limitati» mediante misure legislative per salvaguardare:

- ✓ la sicurezza pubblica,
- ✓ la prevenzione e l'accertamento dei reati,
- ✓ obiettivi di interesse pubblico generale,
- ✓ la tutela dell'interessato o dei diritti e delle libertà altrui,
- ✓ etc…

Torna al sommario

Ambito territoriale

L'ambito territoriale della normativa si amplia, il GDPR si applica al trattamento effettuato:

- ✓ nell'ambito delle attività di uno stabilimento del titolare o del responsabile svolte in Europa
- ✓ sui dati dell'interessato che risiede nel territorio europeo; **Social network, piattaforme web e motori di ricerca saranno quindi soggetti alla normativa europea anche se sono gestiti da società con sede fuori dall'UE.**

Torna al sommario

Formazione

Il Regolamento impone che tutte le persone che trattano i dati debbano:

- ✓ essere **istruiti** in tal senso
- ✓ dimostrare di **conoscere gli adempimenti privacy**.

Torna al sommario

Conclusioni

Bene! Hai concluso la sezione dedicata a PERSONE E RUOLI.

Prosegui con il corso, puoi ora affrontare la sezione **Processi e documenti.**

Torna al sommario