Progettato e realizzato da

Commissionato da

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

commissionato da Università degli Studi di Torino

progettato e realizzato da CSI Piemonte

Modulo 1 – Processi e documenti

Sommario

Obiettivi

In questa seconda sezione dedicata alle novità del GDPR – ambito di intervento **Processi e Documenti** – analizziamo le seguenti tematiche:

- ✓ **Accountability**
- ✓ **Informativa e consenso**
- ✓ **Registro dei trattamenti**
- ✓ **Analisi dei rischi**
- ✓ **DPIA**
- ✓ **Privacy by design**
- ✓ **Privacy by default**
- ✓ **Trasferimenti all'estero**

Torna al sommario

Accountability: responsabilizzazione documentata

Il concetto di **accountability** introduce **il dovere, per il titolare,** di adottare **comportamenti proattivi** e tali da dimostrare l'adozione di misure tecniche ed organizzative finalizzate ad assicurare una concreta compliance normativa.
Deve **giustificare** le ragioni che hanno portato alla **scelta discrezionale delle misure** e ad un giudizio di «**adeguatezza**» rispetto ai rischi per i diritti e le libertà delle persone fisiche.

Deve dimostrare che i trattamenti rispettano i principi generali (liceità, correttezza, trasparenza, finalità determinata, minimizzazione dei dati, conservazione per il tempo necessario a raggiungere la finalità, ecc.).

Torna al sommario

Informativa

Nel momento in cui vengono raccolti i dati (art. 13 - o entro un mese art. 14) **deve essere fornita l'Informativa.**

Vediamone le caratteristiche:

1. L'informativa deve essere:

- ✓ leggibile
- ✓ comunicativa (esempio utilizzo di icone)
- ✓ accessibile
- ✓ corretta
- ✓ trasparente
- ✓ espressa con un linguaggio chiaro e semplice

2. L'informativa deve contenere:

- ✓ l'identità e i dati di contatto del titolare e del DPO
- ✓ le finalità perseguite
- ✓ gli eventuali destinatari dei dati
- ✓ la base giuridica che legittima il trattamento
- ✓ il periodo di conservazione dei dati
- ✓ la logica utilizzata in caso di profilazione, l'eventuale trasferimento dei dati verso paese terzi
- ✓ i diritti che spettano all'interessato

3. L'informativa deve essere fornita per iscritto, al limite stratificata.

- ✓ Ad esempio una prima informativa breve che rimanda ad una seconda più completa.

4. L'informativa non deve essere resa:

- ✓ quando l'interessato dispone già delle informazioni
- ✓ quando risulta impossibile o implicherebbe uno sforzo sproporzionato
- ✓ quando i dati devono rimanere riservati conformemente ad un obbligo di segreto professionale

Torna al sommario

Il consenso

Il consenso deve essere libero, specifico e informato.
Vediamone le caratteristiche.

1. **Il consenso deve consistere in un atto positivo inequivocabile**, anche con un'azione positiva: casella da spuntare o qualsiasi altro comportamento concludente (no silenzio, inattività o preselezione di caselle)
2. Il consenso deve essere espresso un esplicito consenso per **ciascuna finalità** perseguita.
3. Il consenso non deve obbligatoriamente essere scritto ma **è necessario dimostrare di averlo ottenuto.**

Torna al sommario

Il registro dei trattamenti

Il Registro dei trattamenti è il 1° documento a dimostrazione del principio dell'**accountability** e deve essere messo a disposizione dell'Autorità di controllo in caso di richiesta.

Chi deve tenere il registro dei trattamenti

Tutti i Titolari e i Responsabili:

- ✓ con più di 250 dipendenti o
- ✓ che effettuano trattamenti non occasionali a rischio per i diritti e le libertà delle persone fisiche o
- ✓ che effettuano trattamento di dati particolari o relativi a condanne penali e a reati.

Cosa deve contenere il registro dei trattamenti

Il Registro del Titolare deve contenere:

- ✓ il nome e i dati di contatto del titolare del trattamento
- ✓ I dati del DPO
- ✓ le finalità del trattamento
- ✓ le categorie di interessati e di dati personali
- ✓ le categorie di destinatari a cui i dati personali possono essere comunicati
- ✓ gli eventuali trasferimenti di dati personali verso paesi terzi
- ✓ i termini ultimi previsti per la cancellazione delle diverse categorie di dati
- ✓ una descrizione generale delle misure di sicurezza tecniche e organizzative applicate

Un Registro sostanzialmente analogo deve essere tenuto da ogni Responsabile.

A cosa serve il registro dei trattamenti

Il Registro dei Trattamenti, che ricorda l'abrogato Documento Programmatico della Sicurezza previsto dal Codice privacy fino al 2012, risponde quindi alle seguenti **finalità**:

- consente di **tracciare le operazioni di trattamento** effettuate all'interno della singola organizzazione,
- costituisce uno **strumento operativo di lavoro per censire in maniera ordinata le banche dat**i e gli altri elementi rilevanti di ciascun trattamento,
- **rappresenta un documento probatorio** mediante il quale il Titolare o il Responsabile può dimostrare di aver adempiuto alle prescrizioni del Regolamento, nell'ottica del principio di accountability.

Raccomandazioni del Garante

Tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, dovrebbero compiere i passi necessari per **dotarsi di un registro dei trattamenti** al fine di avere uno **strumento che consenta un'accurata ricognizione dei trattamenti** svolti e delle rispettive caratteristiche, e dovrebbero arricchirlo di informazioni ulteriori oltre a quelli obbligatori previsti dal Regolamento.

Ad esempio: gli applicativi che gestiscono il trattamento, i database, le utenze dei soggetti autorizzati al trattamento, ma anche i processi interessati, i fornitori coinvolti.

Torna al sommario

Analisi dei rischi

Il rischio

Con il Regolamento si ha un passaggio dalla pura formalità ad una conformità sostanziale alla protezione dei dati.
Soltanto un **sistema di gestione della data protection**, con un **approccio basato sul rischio** che un trattamento può comportare rispetto ai diritti e alle libertà delle persone fisiche, può concorrere a dimostrare sostanzialmente di essere conformi.
Cos'è il rischio: *il rischio è la **manifestazione di un evento** o di una condizione incerta che, quando si verifica, genera un **effetto (positivo o negativo) su un obiettivo.***

I concetti base

La gestione del rischio (R*isk Management*) è il processo mediante il quale **si misura o si stima il rischio** e successivamente **si sviluppano delle strategie per governarlo.**
Di regola, **le strategie** impiegate includono:
✓ il trasferimento del rischio a terze parti,

- ✓ l'evitare il rischio,
- ✓ l ridurre l'effetto negativo ed infine
- ✓ l'accettare in parte o totalmente le conseguenze di un particolare rischio.

I rischi devono essere valutati in termini di:

- ✓ Riservatezza
- ✓ Integrità del dato trattato
- ✓ Disponibilità

Il rischio è determinato da una matrice che assegna dei valori ai seguenti indicatori:

- ✓ probabilità che l'evento si verifichi
- ✓ gravità dell'impatto che il verificarsi dell'evento potrebbe comportare
- ✓ efficacia dei presidi presenti per mitigare gli eventi

Il processo di Risk Assessment comprende:

- ✓ L'identificazione del rischio
- ✓ L'analisi e la ponderazione del rischio
- ✓ L'identificazione e la valutazione delle opzioni di trattamento
- ✓ La scelta degli obiettivi di controllo e controlli per il trattamento
- ✓ L'accettazione dei rischi residui

I rischi del GDPR

Il GDPR obbliga a valutare i rischi per i diritti e le libertà delle persone fisiche, ossia:

- ✓ *danno fisico, materiale o immateriale*
- ✓ *discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, decifratura non autorizzata*
- ✓ *qualsiasi altro danno economico o sociale*
- ✓ *perdita dei diritti o delle libertà degli interessati*
- ✓ *perdita dell'esercizio del controllo sui propri dati*
- ✓ *valutazione di aspetti personali o profilazione*
- ✓ *dati particolari o giudiziari o dati di persone «vulnerabili»*

- ✓ *considerevole quantità di dati o vasto numero di interessati*

(considerando 75)

Dalla valutazione oggettiva dei rischi deriva:

- ✓ **l'individuazione delle misure tecniche ed organizzative** da porre in essere al fine di mitigare in modo adeguato i rischi
- ✓ **la necessità di redigere la DPIA** e, se il rischio residuo è ancora alto, l'obbligo di procedere con una consultazione preventiva presso l'Autorità
- ✓ **la notifica all'Autorità di controllo di una violazione di dati** (data breach)

Torna al sommario

DPIA – Data Protection Impact Assessment (Art. 35)

Il Titolare deve effettuare una **valutazione d'impatto** sulla protezione dei dati, se il trattamento:

- ✓ prevede l'uso di nuove tecnologie,
- ✓ quando, considerata la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare **un rischio elevato** per i diritti e le libertà delle persone fisiche *(su natura, oggetto e contesto: ad esempio nelle ipotesi di dati raccolti in spazi pubblici o aperti al pubblico, o dati che riguardano soggetti vulnerabili, quali potrebbero essere i minori o i lavoratori con riferimento al trattamento effettuato dal proprio datore di lavoro o dati trasferiti all'estero)*

DPIA: cosa deve contenere

La DPIA contiene almeno:

- ✓ **descrizione** sistematica del trattamento, delle finalità e dell'interesse legittimo perseguito

- ✓ Valutazione della **necessità e proporzionalità** del trattamento rispetto alle finalità
- ✓ Valutazione dei **rischi** per i diritti e le libertà degli interessati
- ✓ Indicazione delle **misure di sicurezza** previste per mitigare i tali rischi ad un livello accettabile

Se i rischi residui (derivanti dall'applicazione delle misure di sicurezza individuate) continuano ad essere **elevati o lo prevede il diritto degli stati europei** (es. compito di interesse pubblico o sanità pubblica), è necessario rivolgersi all'Autorità di Controllo con **una Consultazione preventiva** (art. 36).

Se i rischi cambiano, o almeno ogni 3 anni, è necessario procedere con un riesame della DPIA.

DPIA: quando è richiesta

La valutazione d'impatto è richiesta in particolare nei casi di:

- ✓ Valutazione sistematica e globale[1] di aspetti personali delle persone, basata su un trattamento automatizzato (es. profilazione) e sulla quale si fondano decisioni che hanno effetti giuridici
- ✓ Trattamento su larga scala di dati particolari o giudiziari[2]
- ✓ Sorveglianza sistematica su larga scala di una zona accessibile al pubblico[3]
- ✓ ….. (ulteriore elenco dell'Autorità)

DPIA: quando non è richiesta

La DPIA non deve essere compilata se una norma legittima e disciplina un trattamento necessario per adempiere ad un obbligo legale o

[1] Ad esempio la decisione di concedere o rifiutare un finanziamento basata soltanto sul profilo patrimoniale del richiedente.

[2] Ad esempio un ospedale che conserva i dati particolari dei pazienti, o una compagnia assicurativa rispetto al trattamento di dati personali e particolari dei suoi assicurati.

[3] Ad esempio la sorveglianza di un centro urbano.

necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, ed è stata già fatta una DPIA generale.

Torna al sommario

Privacy by design e privacy by default

Privacy by design

Gli aspetti della riservatezza e della protezione dei dati devono essere valutati **sin dall'inizio** del project design ovvero della progettazione di un sistema informativo che gestisce un trattamento di dati personali (sia un progetto strutturale che concettuale).

Il Titolare deve dimostrare che già dalla progettazione, ovvero dal momento di definire finalità e mezzi del trattamento, ha tenuto in debito conto:

- i principi generali di protezione dei dati (liceità, correttezza, trasparenza, finalità determinata, minimizzazione dei dati, conservazione per il tempo necessario a raggiungere la finalità, ecc.)
- i diritti degli interessati

Privacy by default

Gli aspetti della riservatezza e della protezione dei dati devono essere garantiti – **per impostazione predefinita** – anche durante tutto il ciclo di vita del trattamento.

Il concetto di privacy by default introdotto dal GDPR intende sottolineare la necessità di **tutelare la riservatezza degli interessati** e la protezione dei loro dati «di default» appunto, cioè **come impostazione predefinita.**

Questo implica che il Titolare del trattamento dei dati personali deve trattarli sempre attraverso un percorso di politica aziendale o amministrativa interna che ne garantisca la protezione.

Torna al sommario

Trasferimenti all'estero

È necessario **garantire un elevato livello di protezione anche nel caso in cui i dati vengano trasferiti in un paese terzo** mediante accordi internazionali o decisioni di adeguatezza della Commissione Europea o se vengono fornite **adeguate garanzie agli interessati.**

Torna al sommario

Conclusioni

Bene! Hai concluso le sezioni dedicata a
PERSONE E RUOLI e PROCESSI E DOCUMENTI.
Prosegui con il corso, puoi ora affrontare la sezione **Tecnologie e Strumenti.**

Torna al sommario