ACCREDIA L'Ente Italiano di Accreditamento

Riunione di aggiornamento degli Ispettori ACCREDIA

Aspetti generali del nuovo Regolamento 2016/679 in materia di protezione dei dati personali e impatto sulla documentazione ACCREDIA

Ing. Luca Oldrini
Responsabile per la Protezione dei Dati

Milano
14 settembre 2018

Sommario

- Oggetto della normativa (dati e trattamenti)
- I soggetti coinvolti (Titolare, Responsabili e DPO)
- Informative, consensi e diritti
- La responsabilità del Titolare
- Accountability (responsabilità del Titolare)
- Privacy by design e by default
- Violazione di dati
- Sistema sanzionatorio

Il Regolamento e le normative

- Regolamento Europeo sulla Protezione dei Dati n. 2016/679
- D.Lgs. 196/2003 aggiornato dal D.Lgs. 101/2018 (con entrata in vigore dal 19/09/2018)
- Provvedimenti del Garante

Cosa si intende per dato personale

- Costituisce **dato personale** qualunque informazione idonea ad identificare o a rendere identificabile una **persona fisica** fornendo dettagli sulle sue caratteristiche, abitudini, stile di vita, relazioni personali, stato di salute, situazione economica, ecc…
- I dati personali possono avere diversa natura in base alle informazioni che rivelano. Esistono dati:
    - Identificativi
    - Sensibili (o di categoria particolare)
    - Giudiziari
    - Biometrici
    - Genetici

Cosa si intende per dato personale

- Evidenze di una verifica, persone intervistate, documenti visionati, foto, immagini, mail, ecc…

- Questi sono esempi di dati personali con cui è possibile venire in contatto

Cosa si intende per «trattamento di dati»

- Trattamento è: 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** (art. 4, comma 2).

- I soggetti che procedono al trattamento dei dati personali altrui devono **adottare particolari misure** per garantire il corretto e sicuro utilizzo dei dati.

Cosa si intende per «trattamento di dati»

- Raccogliere e conservare dati su PC o dispositivi, raccogliere documentazioni durante attività di audit, inviare report o informazioni mediante mail, partecipare ad attività di valutazione di pratiche.

- Questi sono esempi di trattamenti che è possibile effettuare durante l'attività.

I soggetti coinvolti nel trattamento di dati

- Il GDPR definisce **caratteristiche soggettive** e **responsabilità** dei soggetti coinvolti nel trattamento dei dati.
- Per quanto concerne le figure di **Titolare** e **Responsabile,** individuate nella legislazione previgente (D.lgs. 196/2003), non vi sono cambiamenti formali. La vera novità introdotta dal GDPR riguarda sostanzialmente gli ***obblighi di dimostrazione*** che la nuova legislazione pone in capo a tali figure.
- In luogo della figura dell'**incaricato**, il GDPR fa riferimento alle «**persone addette al trattamento dei dati**».
- Il GDPR introduce una nuova figura: il **Data Protection Officer** (DPO) con funzioni di **consulenza**, controllo e raccordo con l'autorità di controllo.

Titolare e contitolari del trattamento

- Il **titolare del trattamento** (*data controller*): è la persona fisica, giuridica, pubblica amministrazione o ente che decide il motivo e le modalità del trattamento e risponde giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa in materia di protezione dei dati, sia nazionale che internazionale.
- I **contitolari** (*jointes controllers):* se i titolari sono più di uno il Gdpr consente di nominare i c.d. contitolari del trattamento di cui il rispettivo ambito di responsabilità e i compiti da svolgere devono essere individuati con un apposito atto giuridicamente valido, ai sensi del diritto nazionale.

I soggetti interessati dal trattamento potranno, in ogni caso, esercitare i propri diritti rivolgendosi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente.

I Responsabili del trattamento

- Il **Responsabile del trattamento** dei dati (*data processor*) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento.
- Il GDPR specifica in modo più dettagliato le caratteristiche **dell'atto di designazione** del Responsabile:
  - Deve avere *forma di contratto* o altro atto giuridico vincolante;
  - Deve indicare **la durata, la natura, la finalità** del trattamento, le categorie di dati oggetto di trattamento, le **misure tecniche e organizzative** adeguate a consentire il rispetto delle istruzioni impartite dal titolare;
  - Deve dimostrare che il responsabile fornisca garanzie sufficienti per mettere in atto le misure tecniche e organizzative idonee a garantire la tutela dei diritti dell'interessato.

I Responsabili e Sub Responsabili

- Obblighi specifici del Responsabile:
  - Tenere un registro dei trattamenti svolti;
  - Adottare idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti;
  - Designare il Responsabile per la protezione dei dati (DPO), se tenuto;
  - Se risiede all' esterno dell'UE, designare un rappresentante in Italia quando ricorrono le condizioni previste dal Regolamento.

- I **sub-responsabili:** il GDPR consente al Responsabile di nominare sub-responsabili del trattamento per lo svolgimento di specifiche attività di trattamento. Tali figure sono vincolate ai medesimi obblighi contrattuali che legano titolare e responsabile primario.

Il Responsabile per la Protezione dei Dati

Data Protection Officer (DPO) o Responsabile per la Protezione dei Dati (RPD)

Requisiti:

- Comprovate competenze in ambito giuridico e informatico.
- Può essere una figura interna (dipendente) o esterna (libero professionista, consulente) all'organizzazione e deve conoscerne gli aspetti organizzativi.
- Deve operare in autonomia e assoluta indipendenza.
- Deve essere *tempestivamente e adeguatamente coinvolto* in tutte le questioni inerenti la protezione dei dati e sostenuto nell'esecuzione dei suoi compiti dal titolare e dal responsabile del trattamento che gli devono fornire tutte le risorse necessarie sia per svolgere il suo lavoro.

Il Responsabile per la Protezione dei Dati

Il Responsabile per la Protezione dei Dati (RPD) deve essere un soggetto attivo:

- In caso di problemi è necessario contattarlo (dpo@accredia.it).
- Deve partecipare ad attività di progettazione di nuove attività nelle componenti che riguardano il trattamento di dati personali.
- Deve ascoltare e suggerire modifiche procedurali per aumentare la sicurezza dei dati personali.

DPO: compiti specifici

- L’art. 39 GDPR specifica **i compiti minimi** del DPO:
  - informare e fornire **consulenza** al titolare e al responsabile del trattamento in merito agli obblighi derivanti dal Regolamento 679/2016 o dalle altre disposizioni legislative interne o europee in materia di protezione dati;
  - **sorvegliare** l'osservanza del Regolamento da parte del titolare e del responsabile del trattamento;
  - **cooperare** con l'autorità di controllo, fungendo da punto di contatto tra l’azienda e quest’ultimo.

L’informativa sul trattamento dei dati personali

L’informativa, ai sensi del GDPR, deve indicare anche **informazioni**, necessarie a garantire un trattamento trasparente e corretto:

- Le finalità per cui sono trattati i dati
- I contatti del DPO
- Il trasferimento di dati personali in Paesi terzi
- Il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo
- Il diritto di presentare un reclamo all’autorità di controllo
- Se il trattamento comporta processi decisionali automatizzati
- La base giuridica del trattamento.

Modalità: Forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; linguaggio chiaro e semplice.

Il Consenso; cosa cambia

- **Requisiti:** Libero, specifico, informato e inequivocabile. **Non** è ammesso il consenso tacito o presunto. Per il trattamento di dati sensibili deve essere **esplicito**.
- **Modalità**: Deve essere manifestato attraverso dichiarazione o azione positiva inequivocabile e la **richiesta** deve essere chiaramente **distinguibile da altre** richieste o dichiarazioni rivolte all'interessato.

- Nel caso siano trattati dati di terzi nell'attività di audit è necessario acquisire un consenso anche verbale (foto o raccolta nominativi)
- Il trattamento deve essere pertinente e non eccedente le finalità: se lo stesso obiettivo si raggiunge senza citare nomi o fotografare persone è meglio evitarlo.

I diritti dell'interessato (artt. 15 – 22 GDPR)

- I diritti riconosciuti ai sensi dell'art. 7 Codice Privacy permangono anche con il GDPR. La nuova legislazione definisce in modo più dettagliato il diritto d'accesso ai dati, ampliandolo.
- Il GDPR, poi, accanto ai suddetti diritti ne introduce di nuovi:
  - Diritto di cancellazione (e/o oblio) cd right to be forgotten;
  - Diritto di limitazione del trattamento;
  - Diritto alla portabilità dei dati.

L’obbligo generale di documentazione: Accountability

Art. 5 e Art. 24 GDPR

- Il Titolare deve essere in grado di “**comprovare**” di aver fatto tutto il possibile. Egli ha l’onere di porre in essere una serie di **adempimenti** in modo dimostrabile.
- L’introduzione del concetto di “accountability” determina l’onere di adottare un **nuovo approccio nella gestione della protezione dei dati** da parte delle singole organizzazioni.
- Tutto questo deve avvenire **prima di procedere al trattamento** dei dati e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che **devono sostanziarsi in una serie di attività specifiche e dimostrabili.**

Misure di sicurezza adeguate

Titolare e Responsabile del trattamento devono attuare **misure tecniche ed organizzative adeguate** per garantire un livello di sicurezza adeguato al rischio tenendo conto:

- dello stato dell'arte e dei costi di attuazione,
- della natura,
- del campo di applicazione,
- del contesto e delle finalità del trattamento,
- del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche.

Le misure tecniche ed organizzative di sicurezza da mettere in atto per **ridurre i rischi** del trattamento ricomprendono attività come la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali ecc.

Misure di sicurezza adeguate – aspetti pratici

Titolare e Responsabile del trattamento devono attuare **misure tecniche ed organizzative adeguate**:

- Evitare l'uso di strumenti personali,
- Garantire che gli strumenti utilizzati siano protetti,
- Utilizzare strumenti di comunicazione sicuri.

Le misure tecniche ed organizzative di sicurezza devono essere documentate e validate per dare evidenze oggettive (accountability).

Il registro dei trattamenti

Il Registro delle attività di trattamento svolte dal Comune quale Titolare del trattamento, reca almeno le seguenti informazioni:

- Nome e dati di contatto di Titolare, eventuale contitolare e DPO;
- Finalità del trattamento;
- Categorie di interessati (es. cittadini, residenti, utenti, dipendenti ecc.), categorie di dati personali (dati identificativi, dati relativi alla salute);
- Categorie di destinatari a cui i dati personali possono essere comunicati
- Eventuale trasferimento di dati personali verso un paese terzo od organizzazione internazionale;
- Termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- Richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Privacy by design e by default

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

1. *Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento,* ***sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate****, quali la* ***pseudonimizzazione****, volte ad attuare in modo efficace i principi di protezione dei dati, quali la* ***minimizzazione****, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.*
2. *Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per* ***impostazione predefinita****, solo i dati personali necessari* ***per ogni specifica finalità del trattamento****. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.*
3. *Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.*

La violazione dei dati – Data breach

- Per “**data breach**” si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal titolare.
- Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare **rischi per i diritti e le libertà degli interessati**, dovrà provvedere a **notificare la violazione** all’Autorità di **controllo entro 72 ore** e comunque senza ingiustificato ritardo.
- I principali rischi per i diritti e le libertà degli interessati che possono essere violati a seguito d un data breach sono danni alle persone fisiche, perdita del controllo dei dati personali, limitazione dei diritti, discriminazione, furto o usurpazione di identità, perdite finanziarie, pregiudizio alla reputazione ecc.

La violazione dei dati – Data breach

- Se il Titolare ritiene che il **rischio** per i diritti e le libertà degli interessati conseguente alla violazione **è elevato**, **deve informare gli interessati**, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi.
- I rischi possono essere considerati “elevati” quando la violazione può:
  - coinvolgere **un rilevante quantitativo di dati personali** e/o di soggetti interessati;
  - riguardare **categorie particolari di dati** personali;
  - comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
  - comportare **rischi imminenti e con un’elevata probabilità di accadimento** (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
  - **impattare su soggetti** che possono essere considerati **vulnerabili** per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

La violazione dei dati – Data breach – Aspetti pratici

- In caso di eventi di violazione della sicurezza dei dati:
  - Perdite/furti di supporti informatici
  - Perdite/furti di supporti cartacei
  - Virus su caselle di posta
  - Accesso da parte di soggetti esterni alla propria postazione
- Comunicare l'evento al DPO il prima possibile
- Raccogliere informazioni sull'evento e sui dati che sono stati compromessi

Il sistema sanzionatorio del GDPR

Art. 83 Reg. UE – sanzioni

«…Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione.

Tali sanzioni devono essere effettive, proporzionate e dissuasive.

- Fino a 10 milioni o al 2% del fatturato mondiale (se superiore)
- Fino a 20 milioni o al 4% del fatturato mondiale (se superiore).

Aggiornamento documenti

Aggiornamento dei documenti:

- Convenzione di accreditamento per i CAB
- Aggiornamento convenzione quadro Ispettori/Esperti Tecnici ACCREDIA
- Aggiornamento clausola trattamento dei dati personali e riservatezza per i contratti con i collaboratori
- Informativa per il personale interno e per gli Organi Istituzionali di ACCREDIA

ACCREDIA L'Ente Italiano di Accreditamento

Grazie per l'attenzione

www.accredia.it

info@accredia.it

Dipartimento Certificazione e Ispezione

Dipartimento Laboratori di prova

Dipartimento Laboratori di taratura