PERCORSO OSS

LEZIONE 11

Videolezione 11.4 – I princìpi chiave del GDPR: sicurezza, valutazione del rischio e “data breach”

Introduzione

Il GDPR, di cui abbiamo già parlato più volte, dedica una parte importante a:

- la sicurezza dei dati;
- la valutazione del rischio;
- e alle misure che vanno prese se si verifica una violazione dei dati personali.

In questa lezione vedremo questi tre aspetti sempre considerando che il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili. Insomma, piuttosto che indicare regole minuziose, si è preferito definire principi, ruoli e responsabilità.

La sicurezza dei dati

Il GDPR stabilisce che i dati personali devono essere "trattati in maniera da garantire un’adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale («integrità e riservatezza»)".

È importante notare che è l'intero trattamento a dover essere sicuro, non solo i dati come prodotto finale. Ciò comporta anche che le valutazioni di sicurezza vanno sviluppate per ogni tipo di trattamento.

Le misure di sicurezza, quindi, devono essere adeguate, imponendo non un'obbligazione di risultato, bensì un'obbligazione di mezzi, in modo che le misure siano ragionevolmente soddisfacenti alla luce delle conoscenze e delle prassi.

Le misure di sicurezza si dividono in due categorie: misure tecniche e misure organizzative.

Vediamole in dettaglio…

Per quanto riguarda le misure tecniche, queste comprendono:

- la pseudonimizzazione e la cifratura dei dati personali;

Per quanto riguarda, le misure organizzative, queste comprendono:

- la capacità di assicurare su base permanente la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l’accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l’efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

© 2019 FUNZIONE PUBBLICA CGIL Formazione Concorsi.
Tutti i diritti riservati

Sicurezza dal punto di vista organizzativo

Da quanto appena detto, si intuisce che la sicurezza non riguarda solo l'aspetto informatico del trattamento, ma anche l'aspetto organizzativo volto a coprire eventi quali la sottrazione o la perdita di documenti. Le misure di sicurezza, quindi devono garantire che:

- i dati possano essere consultati, modificati, divulgati o cancellati solo dalle persone autorizzate a farlo (e che tali persone agiscano solo nell'ambito dell'autorità che gli viene concessa);
- i dati trattati siano accurati e completi in relazione al motivo per cui sono elaborati;
- i dati rimangano accessibili e utilizzabili, cioè, in caso di perdita, modifica o distruzione accidentale, si deve essere in grado di recuperarli e prevenire danni alle persone interessate, predisponendo un opportuno piano di continuità operativa.

Il principio di sicurezza, quindi, prevede l'obbligo di riservatezza, integrità e disponibilità dei dati.

Valutazione del rischio

Il Regolamento europeo ha un approccio basato sulla valutazione del rischio, piuttosto che sulla protezione dell'utente. Per cui occorre una corretta analisi del rischio nel trattamento dei dati personali per poter implementare le misure di sicurezza adeguate.

Ecco alcuni tipi di rischio:

- distruzione o perdita di dati;
- modifica;
- divulgazione non autorizzata;
- accesso, in modo accidentale o illegale, non autorizzato.

Per ogni rischio occorre:

- individuare la probabilità dell'evento (la minaccia);
- valutare la gravità dello stesso (l'impatto);
- valutare la qualità dei controlli (adeguatezza) in modo da stabilire le misure di sicurezza adeguate a mitigare il rischio.

Le misure fisiche e logiche di sicurezza

Come abbiamo detto, né il GDPR, né il codice italiano che lo ha recepito indicano esattamente quali misure prendere per la sicurezza. È opportuno però, anche a titolo di esempio, fare un cenno alle misure principali che sono fisiche e logiche (o informatiche).

Parliamo di sicurezze fisiche per misure come:

- il controllo della qualità delle porte e delle serrature e la protezione dei locali con allarmi;
- la limitazione all'accesso ai locali e il controllo dei visitatori;
- il corretto smaltimento dei rifiuti cartacei o elettronici;
- la sicurezza delle apparecchiature informatiche, in particolare i dispositivi mobili.

Parliamo di sicurezza informatica per misure quali:

- sicurezza della rete e dei sistemi di informazione attraverso sistemi di autenticazione;
- sicurezza dei dati conservati nel sistema;
- sicurezza online (sito web o applicazioni online);

© 2019 FUNZIONE PUBBLICA CGIL Formazione Concorsi.
Tutti i diritti riservati

- sicurezza dei dispositivi, in particolare quelli personali, se usati per motivi aziendali.

I sistemi di autenticazione devono essere configurati in modo da controllare gli accessi ai dispositivi e agli applicativi, tramite credenziali (username e password).

Data breach

Una violazione dei dati o, come spesso si chiama in inglese, un "data breach" è una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

Alcuni possibili esempi:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Il titolare del trattamento (soggetto pubblico, impresa, associazione, partito, professionista, ecc.) senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche.

Vanno notificate unicamente le violazioni di dati personali che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali.

Cosa si intende per dati personali

Prima di concludere è importante richiamare cosa si intende per dati personali e quali sono le parti in gioco.

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni su:

- le sue caratteristiche;
- le sue abitudini;
- il suo stile di vita;
- le sue relazioni personali;
- il suo stato di salute;
- la sua situazione economica;
- ecc.

Particolarmente importanti sono:

- i dati che permettono l'identificazione diretta - come i dati anagrafici (ad esempio nome e cognome), le immagini, ecc. - e i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);

© 2019 FUNZIONE PUBBLICA CGIL Formazione Concorsi.
Tutti i diritti riservati

- i dati rientranti in particolari categorie (c.d. "sensibili"), cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale;
- i dati relativi a condanne penali e reati (c.d. dati "giudiziari"), cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

Le parti in gioco

Per quanto riguarda, infine, le parti coinvolte, si distinguono tre figure chiave:

- **Interessato**. È la persona fisica alla quale si riferiscono i dati personali. Quindi, se un trattamento riguarda, ad esempio, l'indirizzo, il codice fiscale, ecc. di Mario Rossi, questa persona è l'interessato;
- **Titolare.** È la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, ecc., che adotta le decisioni sugli scopi e sulle modalità del trattamento;
- **Responsabile**. È la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo del trattamento dei dati.

Conclusioni

In questa lezione abbiamo visto i criteri di sicurezza dei dati, la valutazione del rischio di una violazione e il comportamento da tenere se sfortunatamente la violazione avviene.

Infin, abbiamo ricordato cosa intendiamo per dati personali e quali sono le parti in gioco nel complesso, ma necessario processo di protezione.

© 2019 FUNZIONE PUBBLICA CGIL Formazione Concorsi.
Tutti i diritti riservati