GDPR E ATTIVITÀ ISPETTIVE
COSA ASPETTARSI E COME ARRIVARE PREPARATI AD UNA VERIFICA ISPETTIVA PRIVACY

13 GIUGNO 2022

UNI
UN MONDO FATTO BENE

Con il patrocinio di
ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

UNITRAIN
Conoscere e applicare gli standard

PRESENTAZIONE

Un tema spesso sottovalutato nell'approfondimento del GDPR è l'aspetto sanzionatorio, previsto dal Regolamento Europeo all'art. 83. Il corso si concentra in particolare sull'attività ispettiva che precede l'eventuale emissione di una sanzione, sui diversi protagonisti dell'ispezione e delle modalità della stessa, per poi approfondire il quadro sanzionatorio a seguito di possibili violazioni. L'impianto teorico e pratico del corso permette di apprendere le logiche sottostanti ai controlli e, allo stesso tempo, di calarsi nella realtà di una verifica ispettiva attraverso l'analisi di casi pratici.

OBIETTIVI

Il corso si prefigge l'obiettivo di fornire ai discenti gli strumenti necessari per affrontare adeguatamente e arrivare preparati ad una verifica ispettiva privacy, attraverso l'analisi dei documenti maggiormente oggetto di verifica e le migliori strategie per rispondere adeguatamente alle richieste del soggetto verificante.

DESTINATARI

- Titolari del trattamento di qualsiasi realtà aziendale, Associazioni, Enti o Studi professionali
- Referenti Privacy
- Consulenti Privacy
- DPO

DOCENTI

LUCA OLDRINI - Esperto in gestione sistemi informatici e IT

ALICE GIOVANNICO- Formatore qualificato e consulente esperto per la privacy

CONDIVIDIAMO IL NOSTRO PATTO D'AULA

-Conosciamoci: iniziamo con un giro di presentazione. Ognuno di noi potrà dire di cosa si occupa, in quale ambito lavora, quali aspettative ha rispetto al corso. Se il corso si svolge da remoto rendiamoci riconoscibili scrivendo il nostro nome e cognome nella nostra finestra di Zoom

-Partecipiamo attivamente e confrontiamoci: il corso è un momento di apprendimento che passa anche dal confronto con il docente e i partecipanti. Facciamo domande, chiediamo chiarimenti, ascoltiamo i contributi di tutti

-Utilizziamo gli strumenti in modo consapevole: se il corso si svolge da remoto teniamo preferibilmente accesa la webcam; silenziamo il microfono quando non stiamo parlando; alziamo la mano per richiedere la parola; usiamo la chat se indicato dal docente. Se il corso si svolge in presenza, alziamo la mano per richiedere la parola

-Stabiliamo insieme le pause e rispettiamole

-Evitiamo distrazioni: per quanto possibile, silenziamo il telefono ed evitiamo di leggere mail o messaggi. Durante le pause avremo modo di gestire eventuali urgenze

-Contribuiamo al miglioramento dei corsi UNITRAIN: al termine del corso, compiliamo il questionario di customer satisfaction e forniamo eventuali suggerimenti di miglioramento

-Per il rispetto della privacy di tutti, non ci è permesso effettuare registrazioni audio, video o acquisire screenshot

IL TEAM UNITRAIN SI IMPEGNA A:

-Inviarvi il materiale didattico

-Elaborare ed inviare l'attestato di partecipazione a chi abbia frequentato almeno il 90% dell'ammontare ore del corso. UNITRAIN si riserva la facoltà di verificare, a campione, l'effettiva partecipazione al corso attraverso appelli intermedi .

Sommario

- Chi effettua i controlli
- Tipologie di controlli
- Le campagne di controlli
- Cosa aspettarsi in un controllo: caso pratico
- Come arrivare preparati: suggerimenti sulle procedure.
- Quadro sanzionatorio: sanzioni amministrative e penali

Chi effettua i controlli

Il Garante ha facoltà di effettuare controlli per mezzo di:

- Proprio corpo ispettivo
- Nucleo Speciale Tutela Privacy e Frodi Tecnologiche (NSTPFT): ispettori specializzati sulle tematiche privacy
- Attività gestite dal NSTPFT :
  - il reperimento di dati ed informazioni sui soggetti da controllare;
  - l'assistenza nei rapporti con le Autorità Giudiziarie;
  - la partecipazione di proprio personale agli accessi alle banche dati, ispezioni, verifiche e alle altre rilevazioni nei luoghi ove si svolge il trattamento;
  - lo sviluppo delle attività delegate o sub-delegate per l'accertamento delle violazioni di natura penale o amministrativa;
  - la contestazione delle sanzioni amministrative rilevate nell'ambito delle attività delegate;
  - l'esecuzione di indagini conoscitive sullo stato di attuazione della citata Legge in settori specifici;
  - la segnalazione all'Autorità di tutte le situazioni rilevanti ai fini dell'applicazione del Codice, di cui venga a conoscenza nel corso dell'esecuzione delle ordinarie attività di servizio.

Nucleo Speciale Tutela Privacy e Frodi Tecnologiche (NSTPFT)

- Nucleo del 2018
- Protocollo d'intesa con Autorità Garante siglato nel 2021
- Ispezioni su soggetti pubblici, privati (anche piccoli privati es. videosorveglianza)

Tipologie di controlli

I controlli effettuati dai soggetti autorizzati possono essere:

- Su attività ispettiva programmata (campagne):
  - Verifiche a sorpresa su una serie di soggetti identificati a priori
  - Accessi per raccolta informazioni
- Su segnalazione, reclamo:
  - Accesso o richiesta scritta per raccolta informazioni
  - Provvedimento esecutivo a seguito di istruttoria
  - (non necessariamente sfociano in un controllo se una segnalazione è anonima)

Chi effettua la segnalazione?

Cittadini

Clienti

Utenti

Dipendenti

Focus sulla richiesta di informazioni

Art.58 GDPR

l'articolo del Reg. Europeo che definisce i poteri dell'autorità di controllo

→ **Art. 157 Codice Privacy - Richiesta di informazioni e di esibizione di documenti** – [*Nell'ambito dei poteri di cui all'articolo 58 del Regolamento, e per l'espletamento dei propri compiti, il Garante può richiedere al titolare, al responsabile, al rappresentante del titolare o del responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti anche con riferimento al contenuto di banche di dati*] > *rischio di procedimento sanzionatorio per omessa risposta*

→ **Art. 158 Codice Privacy - Accertamenti** – [*Il Garante può disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali.*] > *può avvenire o in conseguenza di un'omessa risposta o per necessità di ulteriori accertamenti*

Le campagne di controlli

Il Garante definisce controlli semestrali basati su campagne:

- Aree di intervento ispettivo
- Numerosità dei controlli
- Tematiche da valutare

Ad es. link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9096661

1. limitatamente al periodo gennaio-giugno 2019, l'attività ispettiva di iniziativa curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, è indirizzata:

a) ad accertamenti in riferimento a profili di interesse generale per categorie di interessati nell'ambito di:

trattamenti effettuati dall'ISTAT, per una verifica preliminare sul SIM (Sistema Integrato di Microdati) e altri sistemi informativi statistici come da parere sul programma statistico nazionale del 20 ottobre 2015;

trattamenti di dati personali effettuati per il rilascio dell'identità federata (SPID);

trattamenti di dati personali effettuati da Istituti bancari, con particolare riferimento ai flussi di cui all'anagrafe dei conti;

trattamenti di dati personali effettuati da società per attività di marketing;

trattamenti di dati personali effettuati da Enti pubblici, con riferimento a banche dati di notevoli dimensioni;

trattamenti di dati personali effettuati da società con particolare riferimento all'attività di profilazione degli interessati che aderiscono a carte di fidelizzazione.

Deliberazione del 22 dicembre 2021 - Attività ispettiva di iniziativa curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, limitatamente al periodo gennaio-giugno 2022

a) ad accertamenti in riferimento a profili di interesse generale per categorie di interessati nell'ambito di:

trattamenti di dati personali nei confronti di "fornitori di database";

trattamento di dati personali svolti da piattaforme e siti web in ordine alla corretta gestione dei cookies;

trattamento di dati personali nel settore della c.d. "videosorveglianza";

trattamento di dati da parte di siti di incontri; operatori dell'ambito della c.d. data monetization e da parte di produttori e distributori di smart toys;

algoritmi e intelligenza artificiale in ambito pubblico e privato;

b) ad accertamenti nei confronti di soggetti pubblici e privati, al fine di verificare l'osservanza delle disposizioni in materia di protezione dei dati personali, con particolare riferimento alla corretta individuazione dei titolari e dei responsabili del trattamento, anche in relazione all'utilizzo di app. e altri applicativi informatici; attenzione particolare sarà riservata all'acquisizione di informazioni e dati personali da parte di app istallate sugli smartphone e alla verifica sul corretto trattamento dei dati da parte di app diverse da Verifica C19;

Si tratta di un’ispezione sostanziale:

- Verifica della coincidenza tra quanto dichiarato formalmente e quanto effettivamente esistente/ operativo (es. conservazione dati, consenso)
- Accountability, non solo responsabilizzazione nelle decisioni, ma anche capacità di dimostrare

Cosa aspettarsi in un controllo

- Il controllo prevede un accesso da parte di un gruppo (minimo 2 persone) di finanzieri del Nucleo Privacy.
- Il controllo prevede un foglio di raccolta di informazioni in merito ad un elenco di punti.
- Il controllo richiede di descrivere alcune attività inerenti la richiesta di informazioni.
- Il controllo richiede di esibire documenti ed evidenze.

L'esito del controllo è un verbale: risposte ai punti di richiesta informazioni ed allegati con le evidenze.

Cosa aspettarsi in un controllo: caso pratico

Esempio di controllo su attività di gestione di «fidelity c

Oggetto: *Richiesta di informazioni ai sensi dell'art. 58, comma 1, lettera a) ed e), del Regolamento generale sulla protezione dei dati (UE) 2016/679 (di seguito Rgdp) e dell'art. 157 e 158 del decreto legislativo n. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) (di seguito Codice).*

Con riferimento al trattamento di dati personali effettuato attraverso il rilascio di "*fidelity card*", si invita il soggetto in indirizzo, ai sensi dell'art. 58, c. 1, lettera a) ed e), del *Rgdp* e dell'art. 157 e 158 del *Codice*, a comunicare all'organo incaricato di notificare la presente richiesta:

1) struttura ed organizzazione della società;
2) distribuzione delle funzioni in materia di protezione dei dati personali;
3) presupposti di liceità del trattamento dei dati personali per il rilascio della "*fidelity card*";
4) modalità con la quale viene fornita agli interessati l'informativa di cui agli art. 13 e 14 del *Rgdp* acquisendo copia della relativa documentazione;
5) modalità di acquisizione dei consensi ai sensi degli artt. 7 e 8 del *Rgdp*, per le ulteriori finalità (*marketing* – profilazione – comunicazione dei dati a soggetti terzi) con relativa documentazione;
6) eventuale istituzione del registro dei trattamenti mettendone a disposizione copia dello stesso (art. 30 *Rgdp*);
7) eventuale designazione di responsabili esterni (e/o *sub* responsabili) del trattamento con acquisizione del relativo contratto e designazione (art. 28 del *Rgdp*);
8) eventuale nomina del DPO in relazione agli artt. 37 e segg. del *Rgdp*;
9) soggetti autorizzati ad accedere ai dati personali oggetto del trattamento e documentazione relativa all'istruzione ed alla formazione degli incaricati ed eventuale copia delle nomine a incaricati (art. 29 *Rgdp*);
10) tipologia di profilazione effettuata e descrizione dettagliata del suo funzionamento, con particolare riferimento alle modalità di raccolta, di aggregazione e di analisi dei dati personali della clientela;
11) eventuale utilizzo a fini di profilazione di dati particolari dell'interessato (art. 9 *Rgdp*);
12) tipologia di attività di *marketing* effettuato a seguito della profilazione;
13) numero totale dei soggetti a cui è stata rilasciata la *fidelity card*;
14) il periodo di conservazione dei dati di profilazione personali ovvero i criteri utilizzati per determinare tale periodo;
15) valutazione d'impatto eventualmente effettuata in relazione ai trattamenti dei dati oggetto della profilazione tenendo conto di quanto previsto al riguardo nella delibera del Collegio datata 11 ottobre 2018 (*vgs. doc. web.* 9058979) fornendo gli elementi di tale valutazione;
16) presupposti, ambito e modalità di comunicazione a terzi dei dati, anche in riferimento ad eventuali società controllanti, controllate o collegate ed all'eventuale trasferimento dei dati in paesi non appartenenti all'Unione europea;
17) procedure poste in essere per l'esercizio dei diritti degli interessati (artt. 15 a 22 del *Rgdp*);
18) misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (art. 32 del *Rgdp*) con particolare riferimento a:
    - eventuale pseudonimizzazione e cifratura dei dati personali;
    - capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi del trattamento;
    - 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 ed organizzative al fine di garantire la sicurezza del trattamento;
    - principali applicazioni utilizzate sui sistemi (*client server/web application*);
    - misure idonee per accedere a banche dati (*username* e *password*; *strong authentication*;
    - *audit* effettuato sia internamente che presso eventuali responsabili esterni;
    - eventuali *alert* implementati su sistemi;
    - eventuale *backup* sui dati;
19) eventuali certificazioni (art. 42 del Regolamento).

Eventuali ulteriori documenti utili all'istruttoria dovranno pervenire, entro e non oltre 15 giorni dalla notifica della presente richiesta di informazioni, all'organo incaricato di notificare la presente richiesta, per il successivo inoltro al Garante.

Cosa fare in un controllo

- Contattare il referente o il DPO che deve coordinare l'attività.
- Verificare il foglio di richiesta informazioni.
- Valutare se necessario un supporto legale.
- Fornire risposte concise e circoscritte all'oggetto dell'ispezione.
- Se non si ha certezza della risposta, riservarsi di fornire una risposta scritta successivamente.
- Mostrare solo i documenti rilevanti per l'ispezione, fornendoli in copia e non in originale.
- Verificare sempre quanto verbalizzato dagli ispettori.
- Se un'attività ispezionata non è idonea, definire subito un piano di azioni correttive e presentarlo.

Cosa aspettarsi in un controllo: caso pratico

I punti della richiesta:

1) struttura ed organizzazione della società;
2) distribuzione delle funzioni in materia di protezione dei dati personali;

Rappresentare la **struttura dell'organizzazione** in modo schematico per far comprendere come le attività siano svolte per il trattamento oggetto della richiesta di informazioni.

Un **organigramma** aiuta.

Definire in modo chiaro e netto chi è il **titolare del trattamento**: su di esso sono definiti gli obblighi.

Cosa aspettarsi in un controllo: caso pratico

I punti della richiesta:

3) presupposti di liceità del trattamento dei dati personali per il rilascio della "*fidelity card*";
4) modalità con la quale viene fornita agli interessati l'informativa di cui agli art. 13 e 14 del *Rgdp* acquisendo copia della relativa documentazione;
5) modalità di acquisizione dei consensi ai sensi degli artt. 7 e 8 del *Rgdp*, per le ulteriori finalità (*marketing* – profilazione – comunicazione dei dati a soggetti terzi) con relativa documentazione;

Avere definito un elenco dei punti in cui viene raccolto il dato, fornita l'informativa e la modalità di acquisizione del consenso in schemi procedurali aiuta.

Vengono acquisiti i testi delle informative e dei consensi (siano essi su moduli o su form).

Cosa aspettarsi in un controllo: caso pratico

I punti della richiesta:

6) eventuale istituzione del registro dei trattamenti mettendone a disposizione copia dello stesso (art. 30 *Rgdp*);

Il registro deve essere presentato in forma cartacea.

Attenzione a definire la data di redazione e la data di aggiornamento.

Cosa aspettarsi in un controllo: caso pratico

I punti della richiesta:

7) eventuale designazione di responsabili esterni (e/o *sub* responsabili) del trattamento con acquisizione del relativo contratto e designazione (art. 28 del *Rgdp*);

Avere un **elenco dettagliato dei responsabili** e avere una registrazione dell'accordo presente con il responsabile aiuta.

E' necessario verificare i **contratti** con i responsabili.

E' necessario verificare le **autorizzazioni** ai sub-responsabili.

Cosa aspettarsi in un controllo: caso pratico

I punti della richiesta:

8) eventuale nomina del DPO in relazione agli artt. 37 e segg. del *Rgdp*;
9) soggetti autorizzati ad accedere ai dati personali oggetto del trattamento e documentazione relativa all'istruzione ed alla formazione degli incaricati ed eventuale copia delle nomine a incaricati (art. 29 *Rgdp*);

Il DPO, se presente, deve partecipare alla verifica. Il DPO deve avere un incarico scritto o un contratto di servizio.

E' bene avere a disposizione:

- Le nomine degli addetti o incaricati
- Il materiale utilizzato per la formazione
- Un processo di verifica dell'apprendimento

Cosa aspettarsi in un controllo: caso pratico

I punti della richiesta:

10) tipologia di profilazione effettuata e descrizione dettagliata del suo funzionamento, con particolare riferimento alle modalità di raccolta, di aggregazione e di analisi dei dati personali della clientela;
11) eventuale utilizzo a fini di profilazione di dati particolari dell'interessato (art. 9 *Rgdp*);

E' necessario avere una definizione operativa del trattamento con dettaglio delle attività (presenti nel registro).

Nel caso specifico: avere ben definito il concetto di profilazione (art. 4 GDPR)

4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Cosa aspettarsi in un controllo: caso pratico

I punti della richiesta:

12) tipologia di attività di *marketing* effettuato a seguito della profilazione;
13) numero totale dei soggetti a cui è stata rilasciata la *fidelity card*;

E’ necessario avere una definizione operativa del trattamento con dettaglio delle attività (presenti nel registro).

Il livello di dettaglio della descrizione del trattamento è importante: definire mezzi e strumenti utilizzati collegandoli all’elenco dei sistemi informatici (assets)

Cosa aspettarsi in un controllo: caso pratico

I punti della richiesta:

14) il periodo di conservazione dei dati di profilazione personali ovvero i criteri utilizzati per determinare tale periodo;
15) valutazione d'impatto eventualmente effettuata in relazione ai trattamenti dei dati oggetto della profilazione tenendo conto di quanto previsto al riguardo nella delibera del Collegio datata 11 ottobre 2018 (*vgs. doc. web.* 9058979) fornendo gli elementi di tale valutazione;

E' necessario avere una definizione operativa del trattamento con il periodo di conservazione o il criterio che lo determina (presenti nel registro).

Per la valutazione d'impatto verificare quanto previsto nella tabella dei trattamenti obbligati del Garante.

https://www.garanteprivacy.it/documents/10160/0/ALLEGATO+1+Elenco+delle+tipologie+di+trattamenti+soggetti+al+meccanismo+di+coerenza+da+sottoporre+a+valutazione+di+impatto.pdf/b9ceefa9-dd65-df86-fed4-df3c3570f59d?version=1.11

Cosa aspettarsi in un controllo: caso pratico

I punti della richiesta:

16) presupposti, ambito e modalità di comunicazione a terzi dei dati, anche in riferimento ad eventuali società controllanti, controllate o collegate ed all'eventuale trasferimento dei dati in paesi non appartenenti all'Unione europea;

Queste informazioni, così come i punti precedenti (10, 11, 12, 14) devono essere coerenti con l'informativa rilasciata in fase di raccolta dati e con lo schema di raccolta dei consensi.

Cosa aspettarsi in un controllo: caso pratico

I punti della richiesta:

17) procedure poste in essere per l'esercizio dei diritti degli interessati (artt. 15 a 22 del *Rgdp*);

Viene richiesta una descrizione operativa.

Vengono richieste evidenze a campione sulla procedura di gestione e sulla sua conclusione: da quando ricevo la richiesta a quando la evado rispondendo all'interessato.

Cosa aspettarsi in un controllo: caso pratico

I punti della richiesta – aspetti tecnologici:

18) misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (art. 32 del *Rgdp*) con particolare riferimento a:
   - eventuale pseudonimizzazione e cifratura dei dati personali;
   - capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi del trattamento;
   - 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 ed organizzative al fine di garantire la sicurezza del trattamento;
   - principali applicazioni utilizzate sui sistemi (*client server/web application*);
   - misure idonee per accedere a banche dati (*username* e *password*; *strong authentication*;
   - *audit* effettuato sia internamente che presso eventuali responsabili esterni;
   - eventuali *alert* implementati su sistemi;
   - eventuale *backup* sui dati;
19) eventuali certificazioni (art. 42 del Regolamento).

Viene richiesta una relazione descrittiva, non vengono chieste evidenze.

Violazioni della privacy e il sistema sanzionatorio nel 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).

Violazioni della privacy e il sistema sanzionatorio nel GDPR

2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

b) il carattere doloso o colposo della violazione;

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

g) le categorie di dati personali interessate dalla violazione;

Violazioni della privacy e il sistema sanzionatorio nel GDPR

2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

b) il carattere doloso o colposo della violazione;

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

g) le categorie di dati personali interessate dalla violazione;

Violazioni della privacy e il sistema sanzionatorio nel GDPR

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Sanzioni pecuniarie: soglie

Max10 milioni di euro [fino al 2% del fatturato se superiore a 10 milioni]

- Consenso per minori
- Misure di sicurezza
- Accountability
- Principi di Privacy by Design e by Default
- Adempimenti in generale del Titolare del Responsabile e del Rappresentante
- Gestione Data Breach
- Notifica al Garante Privacy
- Valutazione d’impatto
- Responsabile per la Protezione dei Dati
- Aderenza alle Certificazioni privacy

Sanzioni pecuniarie: soglie

Max20 milioni di euro [fino al 4% del fatturato se superiore a 10 milioni]

- Regole per raccolta e documentazione del Consenso
- Principi di correttezza e liceità dei trattamenti
- Diritti degli Interessati
- Trasferimenti di dati extra UE
- Ordini emessi dal Garante privacy
- Data Breach comunicazione agli Interessati
- Rispetto specifici divieti di trattamenti
- Rispetto obblighi per specifici casi es. dati dei lavoratori nel contesto del rapporto di lavoro)

Sanzioni penale

Rappresentate nell'art. 167 e 167 Bis, Ter del D.Lgs. 196/2003 aggiornato dal D.Lgs. 101/2018

- Art. 167 - Trattamento illecito di dati (trarre profitto per sé a danno degli interessati): reclusione da 6 mesi a 1 anno e 6 mesi; da 1 a 3 anni.
- Art. 167 Bis - Comunicazione e diffusione illecita di dati personali (trarre profitto per sé a danno degli interessati): reclusione da 1 a 6 anni.
- Art. 167 Ter - Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala (trarre profitto per sé a danno degli interessati): reclusione da 1 a 6 anni.
- Art. 168 - Falsità nelle dichiarazioni al Garante ed interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante: reclusione da 6 mesi a 3 anni
- Art. 170 - Inosservanza dei provvedimenti del Garante: reclusione da 3 mesi a 2 anni

Provvedimenti

Non necessariamente i controlli generano sanzioni:

- Provvedimenti con indicazioni di blocco del trattamento
- Misure di contrasto all'illecito
- Richieste di maggiori dettagli o richieste di maggiori misure di sicurezza

Grazie per l’attenzione

UNITRAIN

Conoscere e applicare gli standard

– Via Sannio, 2 – 20137 Milano

02 70024379 - 228 formazione@uni.com www.uni.com