L'impatto per lo studio legale del Regolamento Europeo n. 2016/679 (GDPR)

Avv. Sabrina Salmeri

d&l net

ANORC Professioni

MINDWELL

DATA PROTECTION & SECURITY MANAGEMENT

General Data Protection Regulation

Il *General Data Protection Regulation* (**Regolamento Generale sulla Protezione dei Dati - RGPD)** della UE abroga la Direttiva sulla Protezione dei Dati 95/46/CE (recepita in Italia dalla L. 196/2003, c.d. *Codice Privacy*) e ha lo scopo di **armonizzare le leggi sulla protezione dei dati personali e potenziare la privacy dei cittadini dell'Unione Europea.**

173 Considerando - 99 Articoli

Curiosità: **la parola PRIVACY non compare mai all'interno del testo**

La Delega al Governo (art. 13, L. 163/2017)

Il Governo entro 6 mesi (avrebbe dovuto) emanare uno o più decreti legislativi al fine di:

- **Abrogare** le norme del Codice Privacy incompatibili con il nuovo Regolamento;
- **Apportare modifiche al Codice Privacy** per l'attuazione delle disposizioni del GDPR non direttamente applicabili;
- **Coordinare le disposizioni vigenti** in materia di protezione dei dati con le disposizione previste dal Regolamento;
- Ricorrere, se opportuno, a **provvedimenti attuativi e integrativi emanati dal Garante** per la protezione dei dati personali, volti al perseguimento delle finalità previste dal Regolamento;
- **Adeguare il sistema sanzionatorio penale e amministrativo** alle disposizioni previste.

Prima bozza di Dlgs (21 marzo)

Art. 101

(*Abrogazioni*)

60

1. A decorrere dall'entrata in vigore del presente decreto, il Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196 è abrogato. A decorrere da tale data sono altresì abrogati i commi 1021 e 1024 dell'articolo 1 della legge 27 dicembre 2017, n. 205

Breaking News! 10 maggio 2018

Secondo tentativo!

CAMERA DEI DEPUTATI

N.22

ATTO DEL GOVERNO
SOTTOPOSTO A PARERE PARLAMENTARE

Schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (22)

Riferimenti utili

Garante Privacy italiano (=Autorità di controllo) schede illustrative, linee guida del WP29 (=Comitato europeo), provvedimenti

Garante francese

Garante inglese

Decisioni della Commissione Europea

Provvedimenti della Autorità di controllo europee

Ambito di applicazione materiale

Art. 2

Il Regolamento si applica al trattamento - automatizzato e non automatizzato - di **dati personali contenuti in un archivio o destinati a figurarvi**

Esclusioni:

- Trattamento per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione
- Trattamento effettuati dagli Stati membri nell'esercizio di attività che riguardano la **politica estera e sicurezza comune** (Titolo V, capo 2, TUE)
- Trattamento effettuato da una persona fisica per l'esercizio di **attività a carattere personale o domestico**
- Trattamenti effettuati dalle autorità competenti a fini di **prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni**

Ambito di applicazione territoriale

Art. 3

Il Regolamento si applica a **qualunque trattamento dei dati personali posto in essere da un titolare o da un responsabile che operino nell'ambito dell'Unione,** indipendentemente dal fatto che esso abbia o meno avuto luogo nel territorio dell'Unione.

Si applica al trattamento dei dati personali di **interessati che si trovano nell'Unione, effettuato da un titolare o responsabile NON stabiliti nell'Unione**, quando le attività di trattamento riguardano:

- Offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione
- Il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione

Infine, si applica a **titolari non stabiliti nell'Unione ma sottoposti alla legge nazionale di uno Stato membro in virtù del diritto pubblico internazionale**

Definizioni

Art. 4

Dato personale: *qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato). Ad es. nome, numero di identificazione (C.F.), dati relativi all'ubicazione (GPS), un identificativo online (IP, cookie) o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*.

Trattamento: *qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicata 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*.

Principi generali

Art. 5

a) Liceità, correttezza e trasparenza
b) Limitazione della finalità
c) Minimizzazione dei dati
d) Esattezza
e) Limitazione alla conservazione
f) Integrità e riservatezza
g) Responsabilizzazione (*accountability*)

Principi generali

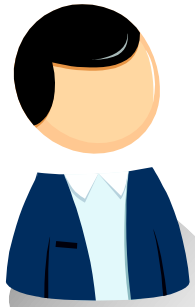
Art. 6

Condizioni per la liceità del trattamento:

a) Consenso
b) Esecuzione di un contratto
c) Adempimento di un obbligo legale
d) Salvaguardia degli interessi vitali dell'interessato di altra persona fisica
e) Esecuzione di un compito di interesse pubblico
f) Perseguimento del legittimo interesse del titolare del trattamento

I soggetti del trattamento

Titolare (Controller)

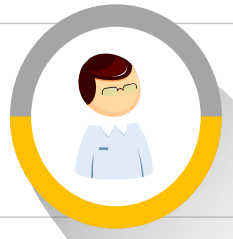


Data Protection Officer

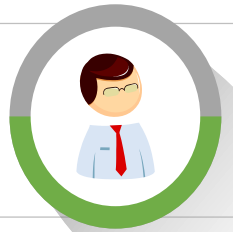
Responsabile
(Processor)

Contitolare

Persona autorizzata



Persona autorizzata



Il titolare del trattamento

Art. 24

1. *Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto* ***misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento****. Dette misure sono riesaminate e aggiornate qualora necessario.*
2. *Se ciò è proporzionato rispetto all'attività di trattamento, le misure di cui al par.1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.*
3. *L'adesione ai codici di condotta di cui all'art. 40 o a un meccanismo di certificazione di cui all'art. 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare.*

Responsabile del trattamento

Art. 28

1. *Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino* ***garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate*** *in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.*

3. *I trattamenti da parte di un responsabile del trattamento sono disciplinati da un* ***contratto*** *o da* ***altro atto giuridico*** ***(scritto, par. 9)*** *a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.*

Persone autorizzate al trattamento

Sono tutte quelle persone che trattano i *dati personali sotto l'autorità diretta del titolare o del responsabile* (art. 4 n. 10).

E' necessario un atto di autorizzazione in cui vengano illustrati l'ambito del trattamento consentito, le istruzioni sulle operazioni di trattamento e sulle misure di sicurezza.

L'obbligo formativo ricade sul titolare che dovrà periodicamente far seguire a tutto il personale corsi di aggiornamento in materia di *data protection*.

Data Protection Officer

Art. 37

Il Responsabile della protezione dei dati, nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:

1. possedere un'**adeguata conoscenza della normativa e delle prassi di gestione dei dati personali**, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze
2. adempiere alle sue funzioni in **piena indipendenza** e in **assenza di conflitti di interesse**. In linea di principio, ciò significa che il DPO non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali
3. operare alle **dipendenze** del titolare o del responsabile oppure sulla base di un **contratto di servizio** (DPO esterno).

Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati le **risorse umane e finanziarie** necessarie all'adempimento dei suoi compiti.

Data Protection Officer

Il Responsabile della protezione dei dati dovrà, in particolare:

a) **sorvegliare** l'osservanza del regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;

b) **collaborare** con il titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);

c) **informare e sensibilizzare** il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;

d) **cooperare con il Garante** e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;

e) **supportare** il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento.

Data Protection Officer

Dovranno designare obbligatoriamente un DPO:

a) **amministrazioni ed enti pubblici**, fatta eccezione per le autorità giudiziarie;

b) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala**;

c) tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di **dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici**.

Anche per i casi in cui il regolamento non impone in modo specifico la designazione di un DPO, è comunque possibile una nomina su base volontaria.

Un gruppo di imprese o soggetti pubblici possono nominare un unico DPO.

Responsabilità

Art. 82

1. ***Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento****.*
2. *Un **titolare** del trattamento coinvolto nel trattamento **risponde per il danno cagionato** dal suo trattamento che violi il presente regolamento. Un **responsabile** del trattamento risponde per il danno causato dal trattamento **solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento**.*
3. *Il titolare del trattamento o il responsabile del trattamento **sono esonerati** dalla responsabilità, a norma del paragrafo 2 **se dimostra che l'evento dannoso non gli è in alcun modo imputabile**.*
4. *Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, **ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.***
5. *Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il **diritto di reclamare** dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento **la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno** conformemente alle condizioni di cui al paragrafo 2.*

Sanzioni

Art. 83

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a ***sanzioni amministrative pecuniarie fino a 10.000.000 di EURO, o per le imprese, fino al 2% del fatturato mondiale totale annuo*** *dell'esercizio precedente, se superiore:*

a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;

b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;

c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4.

Adempimenti

1. Aggiornare l'informativa
2. Riesaminare le politiche interne in tema di trattamento di dati personali
3. Definire i ruoli e redigere le lettere di nomina (responsabile, autorizzato ed eventuale DPO)
4. Registro delle attività di trattamento
5. Valutazione d'impatto (*Data Protection Impact Assessment*)
6. *Security policy* (verifica dei sistemi informatici e adozione di misure adeguate per proteggere i dati da eventuali rischi)
7. Procedure di gestione del *Data Breach*
8. Formare il personale

Informativa

Art. 13

Linguaggio semplice e chiaro

1. I dati di contatto del titolare e del DPO
2. Le finalità e la base giuridica del trattamento
3. Gli eventuali destinatari o categorie di destinatari dei dati personali
4. Il periodo di conservazione dei dati
5. Il diritto di opporsi al trattamento
6. Il diritto di revocare il consenso
7. Il diritto di proporre reclamo all'autorità di controllo
8. Il diritto alla portabilità dei dati
9. L'eventuale trasferimento dei dati in un paese terzo (!)

Informativa

Consiglio Nazionale Forense

☐**esprimo il consenso** ☐**NON esprimo il consenso** al trattamento dei miei dati personali inclusi quelli considerati come categorie particolari di dati.

☐**esprimo il consenso** ☐ **NON esprimo il consenso** alla comunicazione dei miei dati personali d enti pubblici e società di natura privata per le finalità indicate nell'informativa.

☐**esprimo il consenso** ☐ **NON esprimo il consenso** al trattamento delle categorie particolari dei miei dati personali così come indicati nell'informativa che precede.

Diritti dell'interessato

- Accesso (art. 15)
- Rettifica (art. 16)
- Cancellazione/oblio (art. 17)
- Limitazione del trattamento (art. 18)
- Portabilità (art. 20)
- Opposizione (art. 21)

Diritti dell'interessato

1. Il termine per la risposta all'interessato è, per tutti i diritti, **un mese**, estendibile fino a tre mesi per casi di particolare complessità. Il titolare deve comunque dare riscontro all'interessato entro un mese dalla richiesta, anche in caso di diniego.
2. L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato. Ma in caso di richieste manifestamente infondate o eccessive, il titolare può stabilire un eventuale contributo economico da porre a carico dell'interessato.
3. La risposta fornita all'interessato deve essere chiara, concisa, trasparente e facilmente accessibile.

Diritti dell'interessato

Cosa deve fare lo studio legale?

- Assicurarsi di avere una procedura di risposta tempestiva alle richieste dell'interessato/cliente
- Predisporre una procedura di conservazione limitata nel tempo
- Tenere aggiornati i dati degli interessati/clienti
- Procedere a cancellazione sicura dei dati quando non sono più necessari

Registro dei trattamenti

Art. 30

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) **il nome e i dati di contatto del titolare del trattamento** e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del **responsabile della protezione dei dati**;

b) le **finalità** del trattamento;

c) una descrizione delle **categorie di interessati** e delle categorie di dati personali;

d) le **categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i **trasferimenti di dati personali verso un paese terzo** o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i **termini ultimi previsti per la cancellazione** delle diverse categorie di dati;

g) ove possibile, una **descrizione generale delle misure di sicurezza tecniche e organizzative** di cui all'articolo 32, paragrafo 1.

Registro dei trattamenti

Cosa deve fare lo studio legale?

- Redigere il registro
- Esibirlo a richiesta dell'autorità di controllo (Garante)
- Aggiornarlo ove cambino le condizioni in esso contenuto

Valutazione d'impatto (DPIA)

Art. 35

*1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati 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**, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.*

2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

Valutazione d'impatto (DPIA)

Art. 35

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è ***richiesta in particolare nei casi seguenti****:*

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un ***trattamento automatizzato****, compresa la* ***profilazione****, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*

b) il ***trattamento, su larga scala, di categorie particolari di dati personali*** *di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o*

c) la ***sorveglianza sistematica su larga scala*** *di una zona accessibile al pubblico.*

Valutazione d'impatto (DPIA)

Art. 35

7. La valutazione contiene almeno:

*a) una **descrizione sistematica dei trattamenti** previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;*

*b) una valutazione della **necessità e proporzionalità dei trattamenti** in relazione alle finalità;*

*c) una **valutazione dei rischi per i diritti e le libertà degli interessati** di cui al paragrafo 1; e*

*d) le **misure previste per affrontare i rischi**, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.*

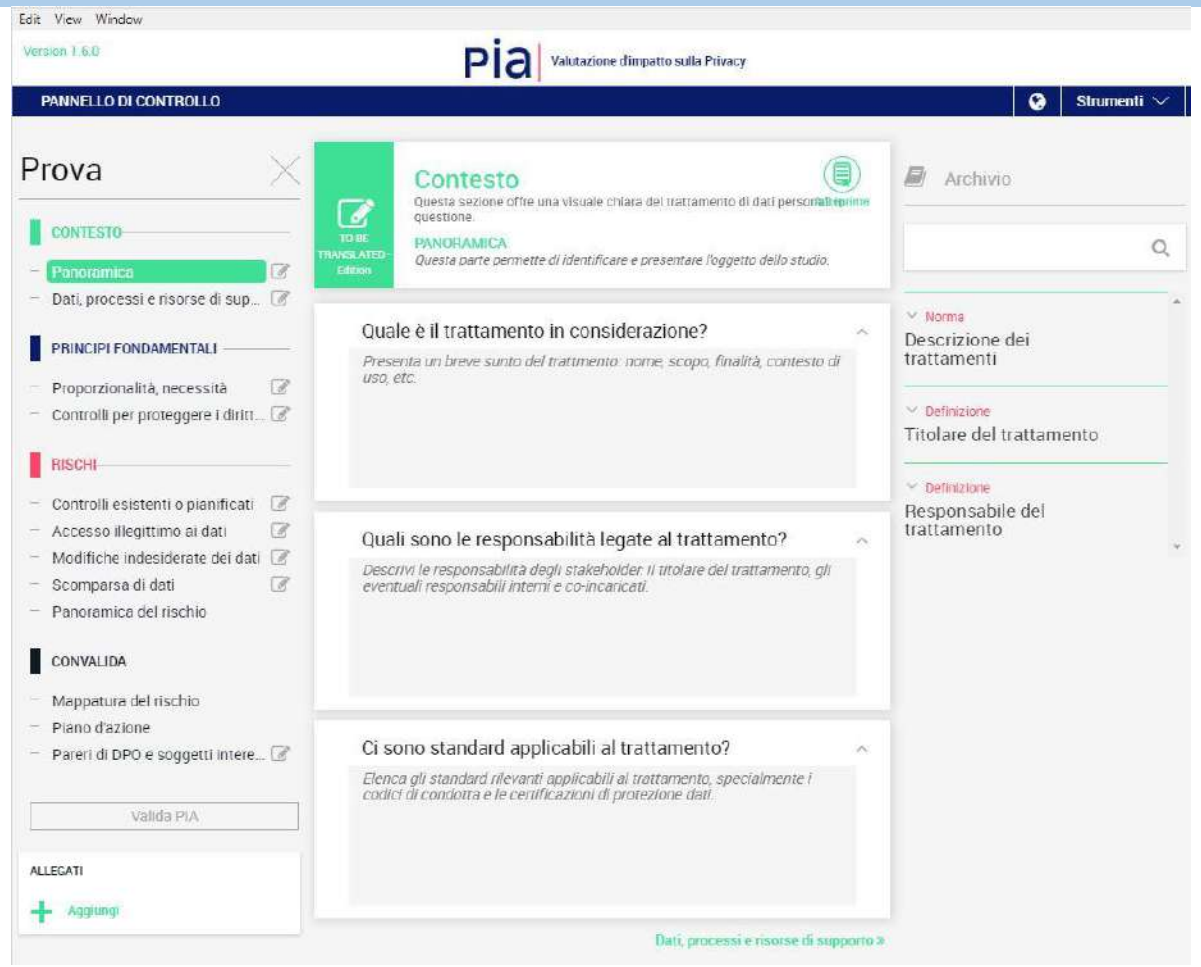
Valutazione d'impatto (DPIA) -> SI

Ospedale	• tratta i dati genetici e sanitari dei propri pazienti (sistema informativo ospedaliero) • dati sensibili o dati aventi carattere estremamente personale • dati riguardanti soggetti interessati vulnerabili • trattamento di dati su larga scala
Autostrade	• L'uso di un sistema di telecamere per monitorare il comportamento di guida sulle autostrade. Il titolare del trattamento prevede di utilizzare un sistema intelligente di analisi video per individuare le auto e riconoscere automaticamente le targhe. • Monitoraggio sistematico; uso innovativo di soluzioni tecnologiche
Azienda->Dipendenti	• Un'azienda che monitora sistematicamente le attività dei suoi dipendenti, controllando anche la postazione di lavoro dei dipendenti, le loro attività in Internet, ecc. • Monitoraggio sistematico • Dati riguardanti soggetti interessati vulnerabili

Valutazione d'impatto (DPIA) -> NO

Singolo medico o avvocato	• trattamento di dati personali di pazienti o clienti • dati sensibili o dati aventi carattere estremamente personale • dati riguardanti soggetti interessati vulnerabili
Rivista online->lista	• utilizza una lista di distribuzione per inviare una selezione quotidiana generica ai suoi abbonati • Trattamento di dati su larga scala
Sito e-commerce->Annunci	• visualizza annunci pubblicitari per parti di auto d'epoca che comporta una limitata profilazione basata sugli articoli visualizzati o acquistati sul proprio sito web • Valutazione o assegnazione di un punteggio

Valutazione d'impatto (DPIA)



https://www.cnil.fr/en/privacy-impact-assessment-pia

Misure tecniche e organizzative

Come proteggere i dati nello studio legale

- Non abbiamo più gli «standard» minimi indicati nell'Allegato B del Codice Privacy tuttavia il Garante, facendo riferimento alle prescrizioni in esso contenute, potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni.
- Il titolare è lasciato libero di scegliere (nel bene e nel male) la tipologie di misure adeguate al tipo di trattamento effettuato e dei dati che tratta.
- Si ricorda che si deve tener presente anche la sicurezza fisica oltre che quella logica.
- Alcune indicazioni le troviamo nel GDPR (art. 32)

Sicurezza del trattamento

Art. 32

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del ***rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche****, il titolare del trattamento e il responsabile del trattamento mettono in atto* ***misure tecniche e organizzative adeguate*** *per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:*

a) la pseudonimizzazione e la ***cifratura*** *dei dati personali;*

b) la capacità di assicurare su base permanente la ***riservatezza****, l'****integrità****, la* ***disponibilità*** *e la* ***resilienza*** *dei sistemi e dei servizi di trattamento;*

c) la capacità di ***ripristinare tempestivamente la disponibilità e l'accesso dei dati personali*** *in caso di incidente fisico o tecnico;*

d) una procedura per ***testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative*** *al fine di garantire la sicurezza del trattamento.*

Esempi di contromisure

Persone

- Formazione sulla sicurezza e consapevolezza
- Controllo del personale

Processi

- Controlli dei sistemi informatici
- Pianificazione della continuità operativa
- Segnalazione e reazione agli incidenti

Prodotto/tecnologia

- Sicurezza fisica e logica
- Protezione da interruzione
- Identificazione e autenticazione

Attenzione!

*"**Protezione dei dati personali**", non equivale a "sicurezza dei dati personali": "proteggere i dati personali" vuol dire proteggere un elemento essenziale dell'essere umano, cioè va inteso – e così è palesemente inteso dal legislatore europeo sin dai Trattati – come diritto fondamentale strumentale alla tutela di altri diritti e libertà fondamentali.*

Avv. Luca Bolognini

*La valutazione d'impatto sulla protezione dei dati svolta ai sensi del regolamento generale sulla protezione dei dati è uno strumento per **gestire i rischi per i diritti degli interessati**, di conseguenza, adotta la loro prospettiva, come avviene in taluni settori (ad esempio, la sicurezza sociale).*
*Al contrario, la gestione del rischio in altri settori (ad esempio in quello della sicurezza delle informazioni) è **incentrata sull'organizzazione**.*

Sicurezza informatica

Data breach

Art. 33

*1. In caso di **violazione dei dati personali**, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.*

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Data breach

Art. 33

3. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Comunicazione di una violazione dei dati personali all'interessato

Art. 34

*1. Quando la violazione dei dati personali è suscettibile di presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.*

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

*3. **Non è richiesta la comunicazione all'interessato** di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:*

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Grazie per l'attenzione!

Avv. Sabrina Salmeri

d&l net

ANORC Professioni

MINDWELL

DATA PROTECTION & SECURITY MANAGEMENT