CNF Consiglio Nazionale Forense

CONSIGLIO NAZIONALE DEGLI INGEGNERI

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

IL DIRITTO ALLA PROTEZIONE DEI DATI E LA TUTELA DELLA PERSONA

Sicurezza, minimizzazione dei rischi, data breach

Dott. Cosimo Comella

Direttore Dipartimento tecnologie digitali e sicurezza informatica

Garante per la protezione dei dati personali

Roma, 17 febbraio 2018

ARGOMENTI

- Aspetti relativi alla sicurezza informatica nel nuovo Regolamento UE

- Il principio della minimizzazione dei rischi
  - Analisi del rischio
  - Predisposizione delle misure di sicurezza e delle azioni mitigatrici

- Quando qualcosa va storto
  - La gestione dei *data breach*
  - Obblighi e opzioni nelle violazioni di dati personali

Il rilievo dato alla sicurezza nel nuovo Regolamento europeo

La sicurezza dei trattamenti nel nuovo Regolamento europeo

Diverse accezioni di «sicurezza»

Nelle premesse:

- Sicurezza pubblica/nazionale/sanitaria/sociale/sul lavoro
- Sicurezza delle reti e dell'informazione
- Sicurezza dei servizi
- Servizi di sicurezza

- **Sicurezza informatica**
- **Sicurezza dei dati personali**
- **Sicurezza del trattamento**
- **Misure di sicurezza**
- **Violazione di sicurezza**

La sicurezza dei trattamenti nel nuovo Regolamento europeo

Considerando 39

I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento.

Considerando 49

Costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi […].

La sicurezza dei trattamenti nel nuovo Regolamento europeo

Considerando 78
(relativo alla «*data protection by design*» e «*data protection by default*»)

[…] Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. […]

Considerando 81
(sul responsabile del trattamento)

Per garantire che siano rispettate le prescrizioni del presente regolamento riguardo al trattamento che il responsabile del trattamento deve eseguire per conto del titolare del trattamento, quando affida delle attività di trattamento a un responsabile del trattamento il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento. […]

La sicurezza dei trattamenti nel nuovo Regolamento europeo

Considerando 83
(relativo alla valutazione del rischio del trattamento)

Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

Previsioni del nuovo Regolamento in tema di sicurezza

La sicurezza dei trattamenti nel nuovo Regolamento europeo

Articolo 5 (Principi applicabili al trattamento di dati personali)

1. I dati personali sono:

[…]
f) 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 accidentali («integrità e riservatezza»).

SICUREZZA TRAMITE TRASPARENZA NEI TRATTAMENTI DI DATI PERSONALI

La documentazione dei trattamenti come elemento della sicurezza

- Importanza della documentazione (tecnica) dei trattamenti con strumenti elettronici
- La documentazione dei sistemi informativi
  - Viste e diagrammi (UML)
  - *Deployment view*
  - Attori interni ed esterni
- L'esperienza del Garante e l'efficacia dell'attività ispettiva
- Prescrizioni in determinati settori
  - Telecomunicazioni
  - Servizi Internet

La documentazione dei trattamenti

Articolo 30 (Registri delle attività di trattamento)

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.

La documentazione dei trattamenti

Articolo 30 (Registri delle attività di trattamento)

2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

   a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
   b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
   c) 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;
   d) ove possibile, una **descrizione generale delle misure di sicurezza tecniche e organizzative** di cui all'articolo 32, paragrafo 1.

La documentazione dei trattamenti

Articolo 30 (Registri delle attività di trattamento)

3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.
4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo
5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

LE MISURE DI SICUREZZA NEL NUOVO REGOLAMENTO EUROPEO

La sicurezza nel nuovo Regolamento

Articolo 32 (Sicurezza del trattamento)

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.

La sicurezza nel nuovo Regolamento

Articolo 32 (Sicurezza del trattamento)

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Le misure di sicurezza informatica

Elencate nell'art. 32 con valore esemplificativo e non esclusivo:

- **Pseudonimizzazione**

  «Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile» (Art. 4 del GDPR)

- **Cifratura**

  Tecnica di protezione crittografica dei dati rilevante per minimizzare i rischi incombenti soprattutto in caso di accessi abusivi o perdita di dati.

Le misure di sicurezza

Valori da tutelare con misure di sicurezza (tecniche e organizzative) adeguate

- Riservatezza (applicazione del principio del «*need to know*»)
  - Sistemi di autenticazione
  - Sistemi di autorizzazione
- Integrità e disponibilità
  - Procedure di *data/disaster recovery*
  - Ridondanza dei dati
- Resilienza dei sistemi e dei servizi di trattamento
  - Tecniche di gestione della «*fault tolerance*»

Le tecniche di anonimizzazione

Anonimizzazione e pseudonimizzazione

- Working Party Art. 29
  Opinion 05/2014 on Anonymisation Techniques
  sulle tecniche di anonimizzazione (10 aprile 2014)
- Elementi essenziali
  - Analisi dell'efficacia e dei limiti delle tecniche disponibili
  - Gestione del rischio residuo di identificazione
  - Riferimento ai «likely reasonably means» per la reidentificazione
  - Randomization/Generalization
    - Noise addition
    - Permutation
    - Differential privacy
    - Aggregation
    - *k*-anonimity
    - *l*-diversity
    - *t*-closeness
  - Pseudonymisation

Le tecniche di anonimizzazione

- Anonymisation techniques can provide privacy guarantees and may be used to generate efficient anonymisation processes, but only if their application is engineered appropriately – which means that the prerequisites (context) and the objective(s) of the anonymisation process must be clearly set out in order to achieve the targeted anonymisation while producing some useful data.
- The optimal solution should be decided on a case-by-case basis, possibly by using a combination of different techniques, while taking into account the practical recommendations developed in this Opinion.
- Data controllers should consider that an anonymised dataset can still present residual risks to data subjects. Indeed, on the one hand, anonymisation and re-identification are active fields of research and new discoveries are regularly published, and on the other hand even anonymised data, like statistics, may be used to enrich existing profiles of individuals, thus creating new data protection issues.
- Anonymisation should not be regarded as a one-off exercise and the attending risks should be reassessed regularly by data controllers.

Le misure minime di sicurezza

Misure minime di sicurezza
(Art. 33-34 e Allegato B del Codice italiano)

- Mancato aggiornamento
- Obsolescenza tecnologica
- *Criminalizzazione* del problema della sicurezza dei dati
- Effetti della c.d. *semplificazione*

Misure minime di sicurezza ICT per la P.A.

- Linee-guida emanate da AgID
  - Ambito applicativo limitato
  - Assenza di sanzioni in caso di disapplicazione

Le misure minime di sicurezza

- Con il nuovo regolamento europeo vengono meno i riferimenti alle c.d. *misure minime di sicurezza* presenti nel Codice italiano

- Possibilità che il Garante reintroduca con propri provvedimenti o linee-guida focalizzate su determinati settori o tipi di trattamento alcuni obblighi aggiuntivi relativi a misure di sicurezza minime.

- Il problema dell'aggiornamento e dell'adeguatezza delle misure
  - Evoluzione tecnologica
  - Mutamenti architetturali
    - Sistemi *on premises*
    - Misure di sicurezza per servizi Cloud computing

I codici di condotta e le certificazioni della protezione dei dati

L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità dei trattamenti al Regolamento anche con specifico riferimento agli aspetti di sicurezza.

Codici di condotta o certificazioni come strumenti a disposizione dei titolari (e dei responsabili) del trattamento per attestare la conformità ai requisiti del Regolamento.

LA MINIMIZZAZIONE DEI RISCHI

La minimizzazione dei rischi

- Sicurezza come percorso, metodo e non come obiettivo tecnico assoluto
- Adeguatezza delle misure di sicurezza rispetto ai rischi incombenti sui dati
- Richiamo alla ragionevolezza delle misure anche sulla base di considerazioni di carattere tecnico ed economico (v. art. 32, comma 1) «Tenendo conto dello stato dell'arte e dei costi di attuazione…»
- Gestione del rischio residuo
  - Mitigazione
  - Assicurazione del rischio
  - Misure di *remediation*
- Minimizzazione dei dati
  - Principio enunciato all'Art. 5 del regolamento: «*I dati personali sono… adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati»* («minimizzazione dei dati»)
  - Meno dati = meno rischi per sé e per gli interessati

L’analisi dei rischi

- È propedeutica alla valutazione delle misure da intraprendere
- Non è una misura nuova, essendo stata prevista per anni quale obbligo e addirittura come «misura minima di sicurezza», nell’ambito del Documento programmatico sulla sicurezza (DPS), anche se riferita al rischio informatico incombente sui dati.
- Deve essere svolta nell’ambito della valutazione d’impatto sulla protezione dei dati (*Data Protection Impact Assessment*) prevista dall’art. 35 del nuovo Regolamento UE (con riferimento ai rischi per i diritti e le libertà degli interessati):

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.

L’analisi dei rischi

- Si tratta di un processo (iterativo) composto da fasi
- Metodologia di analisi non del tutto assimilabile a quella tipica della sicurezza informatica
- Può essere assistito da norme tecniche internazionali (ISO 27005) nel contesto della gestione della sicurezza delle informazioni
- Rischio come relazione tra probabilità che si verifichi un determinato incidente e valutazione del possibile danno da esso derivante
- Nel GDPR il rischio è legato alle libertà e ai diritti degli interessati (*data subjects*)

LA VIOLAZIONE DEI DATI PERSONALI (*Data Breach*)

La violazione dei dati personali

COS'È IL DATA BREACH

(Art. 4 GDPR, definizione 12)
Violazione dei dati personali

«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»

La violazione può essere determinata da accesso abusivo ai sistemi informatici, ovvero da sottrazione o perdita di dati e supporti di memorizzazione.

La violazione dei dati personali

COS'È IL DATA BREACH

- Concetto preesistente al Regolamento GDPR
- Introdotto nelle norme europee con la Direttiva 136/2009 (*Telecom Package*), applicabile al settore delle comunicazioni elettroniche, che ne prevedeva la futura generalizzazione a tutti gli ambiti
- Il nuovo Regolamento UE estende l'obbligo di notificazione dei *data breach* a qualsiasi settore
- L'importanza della trasparenza nei *data breach*
- L'esempio del Nord Europa

La gestione dei *data breach*

OBBLIGHI DEL TITOLARE IN CASO DI DATA BREACH

Articolo 33
(Notifica di una violazione dei dati personali all'autorità di controllo)

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.

La gestione dei *data breach*

CONTENUTO DELLA NOTIFICA DI DATA BREACH

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.

La gestione dei *data breach*

ALTRI ADEMPIMENTI CONNESSI ALLE VIOLAZIONI DEI DATI

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

La gestione dei *data breach*

OBBLIGHI DEL TITOLARE IN CASO DI DATA BREACH

Articolo 34 (Comunicazione di una violazione dei dati personali all'interessato)

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).

La gestione dei *data breach*

QUANDO NON È RICHIESTA LA COMUNICAZIONE

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.

La gestione dei *data breach*

VALUTAZIONE DEL GARANTE

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.

Obblighi del titolare a seguito di violazioni dei dati personali

- In generale, notificare entro 72 ore al Garante l'avvenuto *data breach*

- Non notificare qualora «*sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*»

La notifica di cui al paragrafo deve almeno descrivere
- la natura della violazione dei dati personali
- le categorie e il numero approssimativo di interessati dal breach
- le categorie e il numero approssimativo di registrazioni dei dati personali oggetto di violazione
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto
- le probabili conseguenze della violazione dei dati personali
- 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.

FINE