Workshop «Cybersecurity e mondo finanziario»
Politecnico di Milano, 25 ottobre 2017

LA PROTEZIONE DEI DATI PERSONALI NEL SETTORE BANCARIO

Cosimo Comella <c.comella@gpdp.it>

Dipartimento tecnologie digitali e sicurezza informatica
Garante per la protezione dei dati personali

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Argomenti

- Protezione dei dati nelle banche e negli istituti di credito
- I provvedimenti del Garante sui trattamenti di dati in ambito bancario
- Le novità introdotte dal Regolamento generale sulla protezione dei dati (UE) 2016/679 (GDPR)
  - Nuove definizioni
  - Nuovi concetti
  - Nuovi diritti
  - Nuovi doveri

- Aspetti legati alle tecnologie e alla sicurezza informatica nel GDPR
  - Valutazione dei rischi incombenti sui dati trattati
  - Valutazione d'impatto dei trattamenti
  - Protezione dati «by design» e «by default»
  - Ruoli-chiave della data protection
    - Titolare del trattamento
    - Responsabile del trattamento
    - Responsabile della protezione dei dati (DPO)

Principali criticità nel settore bancario

- Mancata protezione dei dati per carenza o difetti nelle misure di sicurezza
- Comunicazione non autorizzata di dati a terzi
- *Data leakage, data breach*
- Sicurezza delle transazioni bancarie e interbancarie
- Sicurezza dei servizi di *home banking*
- Auditing dei servizi informatici
- Operazioni dispositive e *enquiry*
- Comportamenti discriminatori nella concessione del credito

Principali provvedimenti del Garante rivolti al settore bancario

Provv. 12 maggio 2011 (doc. web n. 1813953) ha esaminato le modalità di circolazione delle informazioni in ambito bancario e fornito prescrizioni in ordine al tracciamento delle operazioni bancarie

Misure necessarie:

- obbligo di registrazione in appositi log delle informazioni riferite alle operazioni bancarie effettuate dagli incaricati sui dati bancari.
- i file di log devono tracciare alcune informazioni (il codice identificativo del soggetto che ha posto in essere l'operazione di accesso, la data e l'ora di esecuzione, il codice della postazione di lavoro utilizzata, il codice del cliente interessato dall'operazione, la tipologia del rapporto contrattuale del cliente cui l'operazione si riferisce);
- i file di log devono essere conservati dalla banca per almeno 24 mesi dalla data di registrazione dell'operazione.
- implementazione di specifici alert che individuano comportamenti anomali e specifiche attività di controllo periodico da parte delle strutture di revisione interna od audit della banca che verifichino anche a posteriori le operazioni effettuate.

Misure opportune:

- raccomandazione alle banche di comunicare al cliente eventuali accessi non autorizzati al proprio conto (eventuali richieste di accesso ai dati avanzate alla banca da clienti che sospettano accessi indebiti ai propri dati bancari da parte di dipendenti, non possono avere ad oggetto i dati riferiti all'incaricato del trattamento che ha effettuato l'accesso, in quanto si tratta di dati riferiti a terzi che come tali non possono essere oggetto di comunicazione (provv. 23 dicembre 2015, doc. web n. 4703279).
- necessità per le banche di rendere note al Garante eventuali violazioni di particolare rilevanza, per quantità, qualità dei dati, numero dei clienti (si tratta della prima applicazione in Italia nel settore bancario del cd. "Data Breach", con il Regolamento Europeo è previsto comunque un obbligo generalizzato di notifica del Data Breach per tutti i titolari del trattamento indipendentemente dal settore di attività e dalla loro dimensione -artt. 33 e 34).

Principali provvedimenti del Garante rivolti al settore bancario

- Rilevazione di impronte digitali ed immagini per accedere agli istituti di credito: limiti e garanzie - 27 ottobre 2005
- Provv. 25 ottobre 2007 «Linee guida per trattamenti dati relativi al rapporto banca-clientela»
- Provvedimenti in materia di firma grafometrica, firma elettronica avanzata e videosorveglianza

Quadro normativo primario

Norme di riferimento vigenti

- Direttiva 95/46/CE (*General Data Protection Directive*)
- Direttiva 2002/58/CE (*ePrivacy Directive*)
- Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196)

Dal 24 maggio 2018

- Piena efficacia delle nuove norme europee:
  - *General Data Protection Regulation (GDPR)*
    Regolamento (UE) 2016/679 del 27 aprile 2016, pubblicato sulla G.U. dell'Unione europea del 4 maggio 2016 (entrato in vigore il 24 maggio 2016, efficace dal 24 maggio 2018)

  - Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, pubblicata sulla G.U. dell'Unione europea del 4 maggio 2016 (entrata in vigore il 5 maggio, da recepire entro il 5 maggio 2018)

Il nuovo regolamento generale europeo sulla protezione dei dati personali (GDPR)

REGOLAMENTO (UE) 2016/679
DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 27 aprile 2016

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)

Le nuove regole europee sulla protezione dei dati personali

- Il "pacchetto protezione dati" si compone di due diversi strumenti:
  - un Regolamento (UE 2016/679) volto a disciplinare i trattamenti di dati personali sia nel settore privato sia nel settore pubblico, che sostituisce la Direttiva 95/46
  - una Direttiva (UE 2016/680) indirizzata alla regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all'esecuzione delle sanzioni penali, che sostituisce la decisione quadro 977/2008, peraltro non ancora attuata dall'Italia
- È stato presentato dalla Commissione il 25 gennaio 2012 e approvato definitivamente dal Parlamento e dal Consiglio il 27 aprile 2016
- I testi definitivi dei provvedimenti componenti il pacchetto sono stati pubblicati sulla Gazzetta ufficiale dell'Unione europea, GU L 119, 4 maggio 2016

Le nuove regole europee sulla protezione dei dati personali

- Il quadro della protezione dei dati personali europea sarà completato con la revisione dell'attuale direttiva ePrivacy (2002/58/CE) su comunicazioni elettroniche e vita privata
  - Nuova direttiva?
  - Nuovo regolamento

Caratteristiche generali del GDPR

- Ambisce a creare un quadro normativo unitario, ma in molti ambiti ammette o rinvia a legislazioni derogatorie degli Stati membri

"*One single law applicable throughout Europe*"

- Possibilità o necessità di specifiche regolamentazioni a livello nazionale in alcune aree lasciate alla competenza delle leggi nazionali
- Mantiene i concetti fondamentali che regolano i ruoli di titolari e responsabili
- Incide e accresce le responsabilità di titolari e responsabili del trattamento
- Incide sul ruolo e i poteri delle *Data Protection Authority* nazionali («autorità di controllo»)

Caratteristiche generali del GDPR

- Testo complesso
  - 173 «considerando»
  - 99 articoli
  - 11 capi
- Struttura del regolamento
  - Capo I – Disposizioni generali
  - Capo II – Principi
  - Capo III – Diritti dell'interessato
  - Capo IV – Titolare e responsabile del trattamento
  - CAPO V – Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali
  - CAPO VI – Autorità di controllo indipendenti
  - CAPO VII – Cooperazione e coerenza
  - CAPO VIII – Mezzi di ricorso, responsabilità e sanzioni
  - CAPO IX – Disposizioni relative a specifiche situazioni di trattamento
  - CAPO X – Atti delegati e atti di esecuzione
  - CAPO XI – Disposizioni finali

CONSENSO

- Per i dati “sensibili” (vedi art. 9 regolamento) il consenso deve essere “esplicito”
- il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22) non deve essere necessariamente “documentato per iscritto”, né è richiesta la “forma scritta”, anche se questa è modalità idonea a configurare l’inequivocabilità del consenso e il suo essere “esplicito” (per i dati sensibili)

INFORMATIVA

- L'informativa (disciplinata nello specifico dagli artt. 13 e 14 del Regolamento) deve essere fornita all'interessato prima di effettuare la raccolta dei dati (se raccolti direttamente presso l'interessato – art. 13)
- Se i dati non sono raccolti direttamente presso l'interessato (art. 14 regolamento), l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento.
- In tutti i casi, il titolare deve specificare la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento (NOTA: ogni volta che esse cambiano il regolamento impone di informarne l'interessato prima di procedere al trattamento), i diritti degli interessati (compreso il diritto alla portabilità dei dati), se esiste un responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati.

INFORMATIVA

- Cosa cambia
  - i contenuti dell'informativa sono elencati in modo tassativo negli articoli 13(1) e 14(1) del Regolamento e in parte sono più ampi rispetto al Codice.
  - il titolare DEVE SEMPRE specificare i dati di contatto del RPD-DPO, ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti
  - ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente"
  - periodo di conservazione dei dati
  - criteri seguiti per stabilire tale periodo di conservazione
  - diritto di presentare un reclamo all'autorità
  - se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato

INFORMATIVA

- Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 regolamento), l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione dei dati (a terzi o all'interessato) (diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice).
- forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile;
- linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee (v. anche considerando 58)
- L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi *online*: vedi art. 12, paragrafo 1, e considerando 58)
- sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1).
- Il regolamento ammette, soprattutto, l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (art. 12, paragrafo 7), e queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.
- Parzialmente diversi i requisiti per l'esonero dall'informativa (vedi art. 13, paragrafo 4 e art. 14, paragrafo 5, oltre a quanto previsto dall'articolo 23, paragrafo 1), anche se occorre sottolineare che spetta al titolare, in caso di dati personali raccolti da fonti diverse dall'interessato, valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato (v. art. 14(5), lettera b)) – a differenza di quanto prevede l'art. 13, comma 5, lettera c) del Codice.

DIRITTI DEGLI INTERESSATI

- Cosa non cambia
  - Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea.
  - Benché sia il solo titolare a dover dare riscontro in caso di esercizio dei diritti (artt. 15-22), il responsabile è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati (art. 28(3), lettera e)).
  - L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni (v. infra).
  - Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee (v. in particolare art. 11, paragrafo 2 e art. 12, paragrafo 6).
  - Sono ammesse deroghe ai diritti riconosciuti dal regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 nonché di altri articoli relativi ad ambiti specifici (in particolare, art. 17, paragrafo 3, per quanto riguarda il diritto alla cancellazione/"oblio", art. 83 - trattamenti di natura giornalistica e art. 89 - trattamenti per finalità di ricerca scientifica o storica o di statistica).
  - Possono continuare a essere applicate tutte le deroghe previste dall'art. 8, comma 2, del Codice in quanto compatibili con le disposizioni citate. Al riguardo, il Garante sta valutando la piena rispondenza delle disposizioni citate in tale articolo del Codice con i requisiti fissati per la legislazione nazionale dall'articolo 23, paragrafo 2, del regolamento.

DIRITTI DEGLI INTERESSATI

- Cosa cambia
  - Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibile fino a 3 mesi in casi di particolare complessità
  - Il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.
  - Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale ragionevole contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) (art. 12.5), a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3)
  - In quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti.
  - Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità;
  - può essere dato oralmente solo se così richiede l'interessato stesso (art. 12, paragrafo 1; v. anche art. 15, paragrafo 3).
  - La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

DIRITTO DI ACCESSO

- Cosa cambia
  - Il diritto di accesso prevede in ogni caso il diritto di ricevere una copia dei dati personali oggetto di trattamento.
  - Fra le informazioni che il titolare deve fornire non rientrano le "modalità" del trattamento, mentre occorre indicare il periodo di conservazione previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi.

Verso il nuovo GDPR

NUOVI CONCETTI E DEFINIZIONI

Nuove definizioni introdotte nel Regolamento europeo

Alcune definizioni introdotte nell'Articolo 4 del Regolamento appaiono formalizzano concetti che erano già presenti e utilizzati senza definizione formale in norme giuridiche

- «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;
- «violazione dei dati personali»: la 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;
- «limitazione di trattamento»: la marcatura di dati personali conservati con l'obiettivo di limitarne il trattamento futuro

Nuove definizioni introdotte nel Regolamento europeo

- «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici
- «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
- «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico

Verso il nuovo GDPR

NUOVI DIRITTI NELLA PROTEZIONE DEI DATI PERSONALI

Evoluzione della protezione dei dati personali europea
Aspetti relativi alla sicurezza

Il diritto all'oblio (o al «delisting»)

Articolo 17

Diritto alla cancellazione («diritto all'oblio»)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
   a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
   b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
   c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
   d) i dati personali sono stati trattati illecitamente;
   e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
   f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

Il diritto all'oblio (o al «delisting»)

Articolo 17
Diritto alla cancellazione («diritto all'oblio»)

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

3. I commi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
   - per l'esercizio del diritto alla libertà di espressione e di informazione;
   - per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
   - per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
   - a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
   - per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il diritto di limitazione del trattamento

Articolo 18
Diritto di limitazione di trattamento

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:
    a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
    b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
    c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
    d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.
2. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
3. L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

La portabilità dei dati

Articolo 20
Diritto alla portabilità dei dati

1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

   a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
   b) il trattamento sia effettuato con mezzi automatizzati.

2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.
3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

Il diritto di opposizione

Articolo 21
Diritto di opposizione

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.
3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.
4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
5. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.
6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Verso il nuovo GDPR

I (NUOVI) DOVERI NEL TRATTAMENTO DEI DATI PERSONALI

Responsabilità del titolare

Articolo 24
Responsabilità del titolare del trattamento

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del 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 e 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.[*cfr. Art. 28 sui responsabili*]

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 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'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Privacy by design/by default

Articolo 25
Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

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

I ruoli nel trattamento dei dati personali

- Art. 26
  Contitolari del trattamento
- Art. 27
  Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione
- Art. 28
  Responsabile del trattamento
- Art. 29
  Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

Verso il nuovo GDPR

LA SICUREZZA DEI TRATTAMENTI NEL NUOVO REGOLAMENTO EUROPEO

La sicurezza dei dati personali 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»).

La documentazione dei trattamenti come elemento della sicurezza

Articolo 30
Registri delle attività di trattamento

1. 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

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.

Aspetti di sicurezza dei trattamenti

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.

Aspetti di sicurezza dei trattamenti

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.

La gestione dei *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.
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*

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

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*

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*

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

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.

Privacy impact assessment

Articolo 35
Valutazione d'impatto sulla protezione dei dati

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

Privacy impact assessment

Articolo 35

Valutazione d'impatto sulla protezione dei dati

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.
5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.
6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

Privacy impact assessment

Articolo 35
Valutazione d'impatto sulla protezione dei dati

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.

Privacy impact assessment

Articolo 35
Valutazione d'impatto sulla protezione dei dati

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.
9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.
10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.
11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

La verifica preliminare dei trattamenti

Articolo 36

Consultazione preventiva (*prior checking*)

1. Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

2. Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

Aspetti di sicurezza dei trattamenti

Articolo 36
Consultazione preventiva (*prior checking*)

3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:
   a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;
   b) le finalità e i mezzi del trattamento previsto;
   c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;
   d) ove applicabile, i dati di contatto del titolare della protezione dei dati;
   e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35;
   f) ogni altra informazione richiesta dall'autorità di controllo.
4. Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento.
5. Nonostante il paragrafo 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.

FINE