Nuovo Regolamento europeo sulla Privacy (679/2016)

FORMA COMUNE – Innovazione Digitale

Asti – 2 Ottobre 2017

La strategia per un approccio unitario alla protezione dei dati personali in Unione Europea

(COM 2010/609)
(COM 2012/09 final)

- Il 4 Novembre 2010 la Comissione Europea ha adottato una comunicazione strategica sulla protezione dei dati personali, mettendo in luce gli obiettivi chiave per la revsione delle norme in vigore.
- La Direttiva del 1995 perseguiva due dei più importanti obiettivi dell'integrazione europea: la protezione dei dati personali come diritto fondamentale e la libertà di circolazione dei dati. Vent'anni dopo, gli obiettivi sono ancora validi ma devono fare I conti con lo sviluppo tecnologico.
- Nel Gennaio 2012, la Commissione Europea ha proposto una complessiva riforma della Direttiva 95/46/EC.
- Il 4 Maggio 2016, il testo ufficiale del Regolamento (e della Direttiva 680/2016) sono state pubblicate nella GUCE.
- Il Regolamento entrerà in vigore il 25 Maggio 2018 e la Direttiva (entrata in vigore il 5 Maggio 2016) dovrà essere attuata entro il 6 Maggio 2018.

Il nuovo Regolamento: esigenze e innovazioni

- Il Nuovo Regolamento affronta le sfide dell'innovazione tecnologica, per offrire nuovi strumenti legali alle esigenze:
  - Della pubblica e globale disponibilità di dati personali nei fenomeni di social networking
  - Della perdita del controllo individuale su informazioni personali potenzialmente sensibili, ad esempio rispetto al "cloud computing"
  - Di crescita nell'utilizzo delle procedure che autorizzano la raccolta automatica di dati personali (ad esempio nella "biglietteria elettronica" o nella geo-localizzazione)
  - della non perfetta consapevolezza delle persone circa I rischi delle nuove tecnologie
  - della perdita di una sufficiente armonizzazione delle legislazioni nazionali
  - Di una corretta allocazione delle responsabilità nel trattamento dei dati personali

La revisione del concetto di «dati personali»

Art. 4

- Il nuovo concetto di "dato personale" ora punta a coprire *ogni informazione correlata a un soggetto identificato o identificabile, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*

Elementi di arricchimento del concetto di «dati personali»

Art. 4

- La *limitazione di trattamento,* consistente nel contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento futuro

- La *pseudonimizzazione,* modalità successiva di trattamento che richiede l'utilizzo di informazioni aggiuntive conservate separatamente e in forma non riconducibile all'interessato, per consentirne la successiva attribuzione al medesimo soggetto

- *(v. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Parere 05/2014 sulle tecniche di anonimizzazione)*

Le novità in merito ai principi

Art. 5

Il regolamento aggiunge il principio di trasparenza, che non era oggetto di disciplina della Direttiva 95/46. La trasparenza riguarda le modalità di *design* e implementazione delle modalità di trattamento

Introduce anche il principio di limitazione delle finalità nei trattamenti successivi (anche di lunga durata) per finalità di ricerca, pubblico interesse o statistica, facendoli soggiacere all'art. 89 del Regolamento (minimizzazione, pseudonimizzazione)

Sostituisce il principio di proporzionalità del trattamento con il principio di minimizzazione rispetto alle finalità del trattamento stesso

L'onere dell'adozione di misure conformi al Regolamento è posto in capo al titolare del trattamento

I principi applicabili al trattamento dei dati personali

Art. 5

- I dati personali devono essere:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

I principi applicabili al trattamento dei dati personali

Art. 5

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

I principi applicabili al trattamento dei dati personali

Art. 5

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

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 liceità del trattamento
Art. 6

- Come già nella Direttiva, anche per il Regolamento Sono condizioni di liceità del trattamento:
  - L'espressione del consenso dell'interessato
  - La necessarietà del trattamento in esecuzione di un contratto o di misure precontrattuali

La liceità del trattamento
Art. 6

- La necessarietà per l'adempimento di un obbligo legale a carico dell'interessato
- La necessarietà per la salvaguardia di interessi vitali dell'interessato
- La necessiarietà per l'esecuzione di un compiuto di interesse Pubblico o connesso all'eseefcizio di pubblici poteri di cui è investito il titolare
- La necessarietà per il perseguimento del legittimo interesse del titolare del trattamernto o di terzi, salva la prevalenza degli interessi o dei diritti dell'interessato, in particolare se è un minore

Le precondizioni per un trattamento trasparente

- trasparenza
- minimizzazione
- controllo

- La trasparenza del trattamento è una condizione indispensabile per esercitare il controllo sui propri dati, quindi le informazioni devono essere facilmente accessibili e comprensibili.
- Per assicurare la garanzia di un alto livello di protezione dei dati personali, occorre che sia garantita la minimizzazione dei dati in relazione allo scopo e la effettiva possibilità per il titolare di disporre del controllo sui propri dati personali.
- Il principio di trasparenza, minimizzazione e ed effetitvo controllo sono già presenti nella legislazione vigente, ma devono essere armonizzati agli ambienti digitali online nei quali i dati personali vengono spesso conservati e trattati all'insaputa dell'interessanto, o senza il suo consenso.

Il principio di trasparenza (considerandum n. 58)

- Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro, oltre che, se del caso, una visualizzazione.
- Tali informazioni potrebbero essere fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito web.
- Dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente.

Le nuove regole sulla trasparenza del trattamento

Art. 12

- Il titolare del trattamento è tenuto ad agevolare l'esercizio dei diritti dell'interessato e non può rifiutare di soddisfare la richiesta dell'interessato, se questa è funzionale all'esercizio dei diritti
- Il titolare deve anche informare l'interessato delle azioni intraprese in seguito a una richiesta di accesso, rettifica o cancellazione.
- Anche l'inottemperanza deve essere comunicata, al più tardi entro un mese dalla richiesta e della possibilità di proporre reclamo o ricorso
- Le attività del titolare sono gratuite, salva l'applicazione di contributi spese di importo ragionevole o la facoltà di rifiuto motivato, nel caso di manifesta infondatezza o eccessiva ripetitività delle richieste.

Le nuove disposizioni sulla minimizzazione e sul controllo dei dati personali nelle piattaforme digitali online

- Il Regolamento introduce l'obbligo di minimizzare i dati trattati ai gestori di piattaforme online e di assicurare all'utente che le impostazioni "di default" non permettano la pubblicazione dei dati.
- Inoltre, i titolari del trattamento dei dati sono esplicitamente obbligati a cancellare dati personali su richiesta, salvo che vi sia un'esigenza legittima alla loro conservazione.
- Per rafforzare I diritti dei titolari, è richiesta la espressa prestazione del consenso al trattamento, sulla base di una esplicita dichiarazione positiva, che deve poter essere data liberamente.
- Se il consenso viene successivamente revocato, I dati devono essere cancellati senza ulteriori azioni da parte dell'utente.

Il principio di minimizzazione (considerandum n. 57)

- Se i dati personali che tratta non gli consentono di identificare una persona fisica, il titolare del trattamento non dovrebbe essere obbligato ad acquisire ulteriori informazioni per identificare l'interessato al solo fine di rispettare una disposizione del presente regolamento.
- Tuttavia, il titolare del trattamento non dovrebbe rifiutare le ulteriori informazioni fornite dall'interessato al fine di sostenere l'esercizio dei suoi diritti.
- L'identificazione dovrebbe includere l'identificazione digitale di un interessato, ad esempio mediante un meccanismo di autenticazione quali le stesse credenziali, utilizzate dall'interessato per l'accesso (log in) al servizio on line offerto dal titolare del trattamento.

Modalità di prestazione del consenso (Art. 7)

- 1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
- 2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.

Revoca del consenso (Art. 7)

- 3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
- 4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Il consenso per i minori (Art. 8)

- Se il trattamento è basato sul consenso, per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.
- Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.

Il consenso per i minori (Art. 8)

- Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.
- Le regole vanno armonizzate con le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore.

Il principio di conservazione del controllo dei dati da parte del titolare (considerandum n. 59)

- Il Regolamento prevede modalità volte ad agevolare l'esercizio, da parte dell'interessato, dei diritti di accesso ai dati, rettifica e cancellazione e per esercitare il diritto di opposizione.
- Il titolare del trattamento deve predisporre anche i mezzi per inoltrare le richieste per via elettronica, in particolare qualora i dati personali siano trattati con mezzi elettronici.
- Il titolare del trattamento è tenuto a rispondere alle richieste dell'interessato senza ingiustificato ritardo e al più tardi entro un mese e a motivare la sua eventuale intenzione di non accogliere tali richieste.

Il principio di conservazione del controllo dei dati da parte del titolare (considerandum n. 60-68)

- L'interessato deve essere sempre informato dell'esistenza del trattamento e delle sue finalità, compresa l'eventuale esistenza di una profilazione e delle conseguenze della stessa.
- In caso di dati personali raccolti direttamente presso l'interessato, questi deve essere informato dell'eventuale obbligo di fornire i dati personali e delle conseguenze in cui incorre se si rifiuta di fornirli.
- Tali informazioni possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto.
- Se presentate elettronicamente, le icone dovrebbero essere leggibili da dispositivo automatico.

Il diritto di accesso ai dati da parte del titolare (considerandum n. 63)

- L'interessato deve avere il diritto di accedere ai dati personali raccolti che lo riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli,
- Ha diritto di ottenere comunicazioni in relazione alla finalità per cui i dati personali sono trattati, ove possibile al periodo in cui i dati personali sono trattati, ai destinatari dei dati personali, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento.
- Il titolare del trattamento deve poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali, senza ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software.

Dati e informazioni garantite dal diritto di accesso (art. 15)

- L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

  a) le finalità del trattamento;

  b) le categorie di dati personali in questione;

  c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

  d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

  e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

Dati e informazioni garantite dal diritto di accesso (art. 15)

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Il principio di rettifica dei dati da parte del titolare e il cd. «diritto all'oblio» (considerandum n. 65)

- Il titolare deve avere il diritto di ottenere la rettifica dei dati personali che la riguardano e il «diritto all'oblio» se la conservazione di tali dati violi il presente regolamento o il diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento.

Il principio di rettifica dei dati da parte del titolare e il cd. «diritto all'oblio» (considerandum n. 65)

- Tale diritto è in particolare rilevante se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet.
- Resta lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

Modalità di esercizio del diritto di rettifica e cancellazione (Art. 16-17)

- L'interessato ha il diritto di ottenere la rettifica e/o l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.
- Il Regolamento fissa uno specifico diritto e l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
  - I dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
  - Il consenso viene revocato non sussiste altro fondamento giuridico per il trattamento;

Modalità di esercizio del diritto di rettifica e cancellazione (Art. 16-17)

- Il titolare si oppone alla prosecuzione del trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento per finalità di marketing diretto;
- Il trattamento è illecito;
- La cancellazione è funzionale all'adempiemento di un obbligo legale
- i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione ai minori.

Estensione a terzi del diritto di rettifica e cancellazione (Art. 16-17)

- Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato 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.

Eccezioni legittime al diritto di cancellazione (Art. 17)

- L'obbligo di cancellazione non si applica:

  a) ai trattamenti necessari per l'esercizio del diritto alla libertà di espressione e di informazione;

  b) per l'adempimento di un obbligo legale che richieda il 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;

  c) per motivi di interesse pubblico nel settore della sanità pubblica;

  d) 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 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;

  e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il diritto alla limitazione del trattamento (Art. 18)

- 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 verificarne l'esattezza;

  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 ha esercitato il diritto di opposizione al trattamento (art. 21), in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Conseguenze della limitazione del trattamento (Art. 18)

- Se il trattamento è limitato, 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.

- L'interessato che ha ottenuto la limitazione del trattamento è informato dal titolare del trattamento prima che detta limitazione sia revocata.

Le nuove tecnologie per la promozione della «privacy fin dall'inizio»

- Il Regolamento introduce il concetto di "Privacy Enhancing Tecnologies" (PET), cioè di tecnologie che garantiscano la privacy fin dallo stadio iniziale del loro sviluppo informatico.

- Nella logica PET è centrale il concetto di "Privacy by Design", cioè di misure di protezione incorporate in tutto il ciclo di vita delle tecnologie e oltre.

La privacy di default (considerandum n. 78)

- il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di 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.

La privacy di default (considerandum n. 78) (Art. 25)

- In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati.

- I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici

Le nuove misure organizzative: i registri delle attività di trattamento (Art. 30)

- Scompare dal Regolamento l'obbligo di notifica dei trattamenti che era previsto dalla Direttiva
- Il titolare del trattamrento deve tuttavia tenere un registro delle attività comprensivo di dati, finalitò, categorie di interessati, categorie di destinatari, termini di cancellazione, descrizione delle misure di sicurezza tecniche e organizzative
- Gli obblighi non si applicano alle organizzazioni con meno di 250 dipendenti, con alcune cautele

Le nuove misure organizzative: la valutazione di impatto (Art. 35)

- 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.

Le nuove misure organizzative: la valutazione di impatto (Art. 35)

- 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.

Le nuove misure organizzative: Il responsabile della protezione dei dati (Art. 37)

- Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

  a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

  b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

  c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

- Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.

Le nuove misure organizzative: Il responsabile della protezione dei dati (Art. 37)

- Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.
- Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.

Le nuove misure organizzative: Il responsabile della protezione dei dati (Art. 37)

- Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.
- Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.
- Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Le nuove misure organizzative: Compiti del responsabile della protezione dei dati (Art. 39)

- Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

  a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

  b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

Le nuove misure organizzative: Compiti del responsabile della protezione dei dati (Art. 39)

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Le regole sulla profilazione dei dati (considerandum n. 71)

La «profilazione» consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona.

La profilazione è un fenomeno rilevante qualora l'interessato venga sottoposto a una decisione basata unicamente su trattamenti automatizzati e che produca effetti giuridici, come nel caso di rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani.

Le regole sulla profilazione dei dati (considerandum n. 71)

Il Regolamento ammette la liceità di trattamenti che includano la profilazione, qualora previsto dal diritto dell'Unione o degli Stati membri, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito.

In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione.
Tale misura non dovrebbe riguardare un minore.

La violazione dei dati personali (considerandum n. 85/87)

Non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento deve notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

La violazione dei dati personali (considerandum n. 85/87)

Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie.

La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge.

Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione.

La violazione dei dati personali (considerandum n. 85/87)

È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato.

È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato.

Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento.

Grazie per l’attenzione