Regione Toscana

VADEMECUM

PRINCIPALI PROFILI DI NOVITÀ APPORTATI DAL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

2018

Luglio

Regione Toscana POR FSE 2014-2020 FONDO SOCIALE EUROPEO
Unione europea Fondo sociale europeo
REPUBBLICA ITALIANA
Regione Toscana

REGIONE TOSCANA

DIREZIONE ORGANIZZAZIONE E SISTEMA INFORMATIVO

SETTORE ORGANIZZAZIONE E SVILUPPO RISORSE UMANE
in collaborazione con
UFFICIO RESPONSABILE PROTEZIONE DATI

Luglio 2018

www.regione.toscana.it/-/regolamento-europeo-sulla-protezione-dei-dati-gli-atti-regionali

Indice

Introduzione

A partire dal 25 maggio 2018 è divenuto direttamente applicabile negli Stati membri il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, in materia di "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", denominato anche "General Data Protection Regulation"[1] (a seguire, anche «GDPR» o «Regolamento»).

Il GDPR tutela il diritto alla **protezione dei dati personali**, al fine di garantire che il **trattamento** degli stessi da parte di terzi sia conforme alle regole e ai principi stabiliti dalla legge.

Il Regolamento mira altresì ad adeguare il quadro normativo vigente al mutato contesto sociale ed economico e ad assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione, nonché a prevenire le disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno.

Per **dati personali**[2], si intendono le **informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica** e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica. Il concetto di dato personale è quindi dinamico e deve essere sempre ricondotto al contesto di riferimento. In concreto, un'informazione isolata spesso non consente di identificare un soggetto, mentre ciò risulta possibile mediante l'integrazione con altri dati. Il criterio dell'identificabilità mediante incrocio di informazioni, anche se detenute da diversi titolari, fa sì che anche i dati online, come gli indirizzi IP e i cookie rientrino nel concetto di dato personale.

Vi sono differenti tipologie di dati personali, che saranno oggetto di trattazione nel successivo paragrafo "Trattamento dei dati personali".

Nello specifico, le previsioni del GDPR prendono in esame l'intero ciclo di **trattamento dei dati personali**[3], meglio descritto nel successivo paragrafo "Trattamento dei dati personali", da intendersi come lo svolgimento di qualsiasi **operazione o complesso di operazioni avente ad oggetto la gestione dei dati personali**, ivi inclusa la raccolta, la protezione, la modificazione, la conservazione e la cancellazione degli stessi.

Il ciclo di trattamento dei dati personali prevede:

---

[1] Il Regolamento UE 679/2016 è reperibile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=IT.

[2] Ai sensi dell'art. 4, n. 1 del GDPR, per dato personale si intende *"qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, 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"*.

[3] Ai sensi dell'art. 4, n. 2 del GDPR, il trattamento dei dati consiste in *"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"*.

Le Pubbliche Amministrazioni effettuano il trattamento dei dati personali nello svolgimento delle proprie attività sia con riguardo a dati acquisiti direttamente dagli interessati (i soggetti ai quali si riferiscono i dati) sia con riguardo a dati forniti da terzi. A titolo esemplificativo, il trattamento avviene nell'ambito di procedure di appalto, concorsi e prove selettive, atti di concessione di sovvenzioni, contributi e sussidi.

L'approccio proposto dal GDPR è orientato al principio di **responsabilizzazione** ("*Accountability*") del titolare/responsabile del trattamento, considerando la protezione dei dati non come un mero obbligo formale e promuovendo la consapevolezza degli interessati sui propri diritti e libertà.

Il **Garante per la protezione dei dati personali** è l'autorità amministrativa indipendente che verifica che il trattamento dei dati avvenga in conformità con le disposizioni normative, esamina reclami, adotta provvedimenti volti a contrastare eventuali violazioni, nonché applica sanzioni in caso di inadempimento degli obblighi in materia e nei casi previsti dalla legge.

Tutto ciò premesso, il presente documento illustra sinteticamente:

- il quadro normativo nazionale di riferimento;
- le diverse figure coinvolte nel trattamento dei dati personali, dedicando una particolare attenzione al DPO, nuovo soggetto introdotto dal GDPR con un ruolo chiave nella promozione della cultura della protezione dei dati;
- il nuovo approccio nel trattamento dei dati ispirato ai principi di "*Privacy by design e by default*" e "*Accountability*";
- il trattamento dei dati personali e le tipologie di dati;
- i nuovi obblighi e le responsabilità in capo alle organizzazioni;
- la valutazione d'impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato";
- le sanzioni previste in caso di inadempimento agli obblighi previsti.

Quadro normativo in materia di protezione dei dati personali

L'attuale quadro normativo in materia di protezione dei dati personali è caratterizzato dalla contestuale applicazione:

- del **Regolamento UE 2016/679**, che, in quanto fonte normativa comunitaria direttamente applicabile, prevale sulla normativa interna con esso non compatibile;
- del **D.Lgs. 30 giugno 2003, n. 196** (a seguire, anche «Codice») nella misura in cui risulta compatibile con le disposizioni del GDPR.

Ad oggi, lo schema di decreto legislativo volto ad adeguare il Codice al Regolamento è ancora in corso di approvazione[4].

Il Regolamento, rispetto al Codice, introduce alcuni aspetti innovativi tra cui: la ridefinizione dei soggetti coinvolti nel trattamento dei dati personali, nonché l'introduzione della nuova figura del DPO e dei relativi compiti loro attribuiti; una maggiore attenzione all'utilizzo dei dati dei minori; il *data breach*; la valutazione d'impatto sulla protezione dei dati; le misure di sicurezza aggiuntive per il trattamento dei dati appartenenti alle categorie speciali; una maggiore rilevanza della finalità del trattamento del dato.

Seppur riprendendo alcuni aspetti già contenuti nel Codice, in sintesi, il Regolamento: i) garantisce la certezza del diritto e la trasparenza agli operatori economici, comprese le micro, piccole e medie imprese; ii) offre alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei Titolari del trattamento e dei Responsabili del trattamento; iii) assicura un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri.

Una delle più rilevanti caratteristiche del Regolamento è il suo ambito di applicazione (art. 3): le disposizioni normative ivi contenute vengono applicate "*[…] indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*".

L'ambito di applicazione si pone infatti in maniera innovativa sotto due profili, ovvero, il Regolamento si applica:

(i) al trattamento dei dati personali effettuato dal titolare o dal responsabile stabilito nell'UE, indipendentemente da dove sia effettuato il trattamento stesso;

(ii) anche a titolari e responsabili di trattamento non residenti nell'UE, al ricorrere di alcune condizioni[5].

Alla luce delle innovazioni rappresentate e al fine di armonizzare il quadro normativo interno rispetto alla normativa comunitaria e di adeguare la normativa nazionale alle disposizione del

[4] Di seguito il link dello schema di decreto in corso di approvazione http://www.senato.it/service/PDF/PDFServer/BGT/1067310.pdf.

[5] Il Regolamento viene applicato ai titolari e responsabili del trattamento non residenti nell'UE al ricorrere delle seguenti condizioni ovvero che: (i) trattino dati personali di persone fisiche che si trovano nell'UE quando il trattamento è in relazione a offerte di beni e servizi, indipendentemente dal fatto che sia richiesto o meno un pagamento; o (ii) effettuino attività di monitoraggio sul comportamento di persone fisiche che si trovano nell'UE nella misura in cui tale comportamento avvenga nell'UE.

GDPR, l'art. 13, comma 3 della Legge 25 ottobre 2017 n. 163 (Legge di delegazione europea 2016-2017) ha delegato il Governo ad adottare uno o più decreti legislativi volti a coordinare le previsioni del D.Lgs. 196/2003 con quelle del GDPR[6].

Il termine per l'attuazione della delega, originariamente previsto per il 21 maggio 2018, è stato automaticamente prorogato di tre mesi, ai sensi dell'art. 31 della Legge n. 234 del 2012, e dunque scadrà il 22 agosto 2018.

Le figure coinvolte nel trattamento dei dati personali

Il GDPR delinea le figure coinvolte nel trattamento dei dati personali e, in particolare, il titolare, i contitolari, il responsabile, il sub-responsabile, la persona autorizzata al trattamento. Di seguito, si riporta una descrizione delle richiamate figure.

Tipologia	Descrizione
Titolare	*"[…] la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali"* (Artt. 4 e 24).
Contitolari	Qualora vi siano due o più titolari del trattamento che determinino congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento (Art. 26). In tal caso, i titolari sono tenuti a definire specificamente con un accordo interno, il rispettivo ambito di responsabilità e i compiti, con particolare riguardo all'esercizio dei diritti degli interessati.
Responsabile del trattamento	"*[…] la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*" (Artt. 4 e 28). Il GDPR precisa che i trattamenti effettuati da parte del responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli stati membri, che, ai sensi dell'art. 28

[6] In particolare, il richiamato articolo prevede che l'armonizzazione debba avvenire secondo i seguenti criteri: *"a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel Regolamento (UE) 2016/679; b) modificare il codice di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel Regolamento (UE) 2016/679; c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal Regolamento (UE) 2016/679; d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal Regolamento (UE) 2016/679; e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del Regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse".*

	par. 3 del GDPR, "*[…] vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*".
Sub-responsabile del trattamento	Soggetto eventualmente nominato dal responsabile del trattamento ai sensi dell'art. 28, par. 4 per lo svolgimento di specifiche attività, fermo restando che "*il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile*".
Persona autorizzata al trattamento dei dati	Persona istruita ed autorizzata dal titolare a trattare i dati personali all'interno dell'organizzazione dello stesso titolare e sotto la sua diretta autorità (Art. 4, n. 10).

Il Data Protection Officer (DPO)

(artt. 37-38-39)

Il GDPR prevede la designazione di un DPO[7], figura che riflette **l'approccio responsabilizzante** proprio del Regolamento (Art. 39).

Il DPO è infatti il soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di controllo e supporto, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo. Il DPO coopera con l'Autorità (e proprio per questo il suo nominativo deve essere comunicato al Garante) e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali.

Il DPO deve possedere specifici **requisiti, competenze professionali e conoscenze specialistiche** richieste alla luce delle funzioni attribuite a tale figura. In particolare, il DPO:

- è designato in funzione delle qualità professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti che allo stesso sono assegnati (art. 37, par. 5);
- deve poter adempiere alle sue funzioni in piena indipendenza (art. 38, par. 3);
- deve poter adempiere alle sue funzioni in assenza di conflitti di interesse, specie qualora svolga altri compiti e funzioni (art. 38, par. 6).

[7] Si vedano, al riguardo, le "Linee guida sui responsabili della protezione dei dati", adottate dal WP29 il 13 dicembre 2016, emendate in data 5 aprile 2017 e reperibili al seguente link: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5930287.

Ai sensi dell'art. 39 del GDPR, il DPO è tenuto a:

- sorvegliare l'osservanza del Regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
- collaborare con il titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);
- informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal Regolamento e da altre disposizioni in materia di protezione dei dati;
- cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;
- supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento.

Al fine di consentire l'efficiente svolgimento dei compiti ai quali è preposto, il DPO deve:

- essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
- poter riferire direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento;
- essere dotato di risorse sufficienti a svolgere in modo efficace i compiti cui è chiamato e a mantenere la propria conoscenza specialistica;
- poter accedere ai dati personali e ai trattamenti.

"Privacy by design e by default" e "Accountability"

(artt. 23-25)

In un'ottica di rafforzamento dei diritti e delle libertà di riservatezza degli interessati e di maggiore responsabilizzazione dei soggetti coinvolti nel trattamento dei dati, il GDPR introduce, tra gli altri, i principi della "***Privacy by design e by default***" e della "***Accountability***".

In particolare, i principi della "***Privacy by design e privacy by default***" impongono al titolare del trattamento di mettere in atto - sia al momento in cui determina i mezzi del trattamento sia all'atto del trattamento stesso - azioni mirate alla protezione dei dati personali al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati prima di procedere al trattamento dei dati.

Il GDPR riconosce, altresì, particolare importanza al principio di ***"Accountability"*** del titolare e del responsabile del trattamento. In conformità con la maggiore "responsabilizzazione" di tali figure, è prevista l'adozione di tutte le misure tecniche ed organizzative necessarie a garantire la protezione dei dati personali nei processi di trattamento degli stessi in conformità con quanto previsto dal quadro normativo vigente.

Trattamento dei dati personali

(artt. 4, n. 1-2; 5; 6; 9; 10)

Ai sensi dall'art. 5 del GDPR, il trattamento dei dati personali deve avvenire nel rispetto dei seguenti principi:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati che consiste nell'adeguatezza, della pertinenza e della limitazione a quanto necessario dei dati rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva rettificazione o cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione ad un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza, consistente nella necessità di garantire la sicurezza dei dati personali - inclusa la protezione attraverso misure tecniche e organizzative idonee allo scopo - riducendo il rischio di trattamenti non autorizzati o illeciti, nonché di perdita, distruzione o danneggiamento accidentale.

La modalità utilizzata per il trattamento dei dati personali è determinata dalla tipologia di dato personale trattato.

In particolare, il Regolamento prevede particolari condizioni per ciò che concerne il trattamento delle categorie particolari di dati e i dati relativi a condanne penali e reati o a connesse misure di sicurezza.

(i) Focus sulle tipologie di dati personali

Le varie tipologie di dati personali sono:

Tipologia	Descrizione
Dati personali comuni	I dati che consentono di identificare direttamente o indirettamente una persona fisica, tra cui, ad esempio, nome e cognome, indirizzo di casa, indirizzo email, numero identificativo nazionale, numero di passaporto, indirizzo IP, numero di targa del veicolo, numero di patente, volto, calligrafia, numeri di carta di credito, identità digitale, data di nascita, luogo di nascita, numero di telefono, nickname. Rientrano tra i dati comuni anche quei dati personali che risultano essere strettamente connessi con l'evoluzione delle nuove tecnologie ovvero i dati relativi alle

	comunicazioni elettroniche via internet o telefono, nonché quelli che forniscono informazioni sui luoghi frequentati e sugli spostamenti (geolocalizzazione). Non rientrano nei dati personali comuni le "Categorie particolari di dati personali" di cui all'art. 9 del GDPR e i "Dati personali relativi a condanne penali e reati" di cui all'art. 10 del GDPR.
Categorie particolari di dati personali[8]	I *"dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica* (quali a titolo esemplificativo, un gruppo di fotografie caricate online, oppure negli aeroporti dove l'immagine dell'individuo viene scansionata per identificarlo)*, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona"* (art. 9 del GDPR).
Dati relativi a condanne penali e reati o a connesse misure di sicurezza	I dati che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato (art. 10 del GDPR[9]).

Nuovi obblighi e responsabilità

Tenuto conto del principio di *accountability,* i Titolari e i Responsabili sono destinatari di nuovi obblighi e responsabilità nello svolgimento delle loro attività, come di seguito descritti:

(i) Registro delle attività di trattamento (Art. 30)

Il titolare del trattamento è tenuto a redigere il Registro di tutte le attività svolte sotto la propria responsabilità.

Tale importante strumento è in grado di fornire, da un lato, un **quadro aggiornato dei trattamenti** effettuati all'interno delle Amministrazioni al titolare e, dall'altro, di consentire un'eventuale **supervisione da parte del Garante** per la protezione dei dati personali.

La tenuta del Registro delle attività di trattamento è parte integrante di un sistema di corretta gestione dei dati personali in quanto consente l'analisi, la ricognizione, la mappatura e la

[8] Si tratta di una nozione più ampia rispetto a quella di c.d. dato sensibile fornita dall'art. 4, comma 1, lett. d) del Codice.

[9] Si tratta dei c.d. dati giudiziari di cui all'art. 4, comma 1, lett. e) del Codice.

valutazione di conformità delle attività di trattamento svolte rispetto a quanto previsto dal Regolamento.

Nello specifico, il Registro deve contenere tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, 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 all'art. 49 par.2 del GDPR, 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'art. 32, par. 1 del GDPR.

(ii) Informativa (Artt. 13- 14)

Il GDPR, rispetto alla disciplina di cui al Codice, amplia i contenuti dell'informativa da rendere agli interessati.
Nello specifico, il GDPR prevede: (i) l'informativa ai sensi dell'art. 13 nei casi in cui i dati personali oggetto del trattamento sono raccolti presso l'interessato; (ii) l'informativa ai sensi dell'art. 14 nei casi in cui i dati non sono stati ottenuti presso lo stesso interessato, ma da fonte diversa.

Informativa ex art. 13 del GDPR

Ai sensi dell'art. 13, il titolare del trattamento è tenuto a fornire l'informativa nel momento in cui i dati sono ottenuti.

Nello specifico, i contenuti dell'informativa sono i seguenti: i) l'identità e i dati di contatto del titolare; ii) i dati di contatto del DPO; iii) le finalità, nonché la base giuridica del trattamento; iv) il proprio interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento; v) l'eventuale trasferimento dei dati personali in Paesi terzi e, in caso affermativo, gli strumenti e le modalità con i quali avverrà tale trasferimento; vi) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; vii) il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione; viii) i diritti degli interessati; ix) il diritto di presentare un reclamo all'autorità di controllo; x) l'eventuale natura obbligatoria del conferimento dei dati.

Se il trattamento comporta processi decisionali automatizzati (ivi compresa la profilazione), l'informativa dovrà contenere una specifica in tal senso, nonché indicare la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Infine, qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di procedere a tale ulteriore

trattamento, fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente.

Informativa ex art. 14 del GDPR

Ai sensi dell'art. 14, l'informativa deve essere fornita all'interessato:

- entro un termine ragionevole e comunque non oltre un mese dalla raccolta dei dati in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
- nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato;
- nel caso in cui sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

Oltre ai contenuti previsti dall'art. 13, l'informativa di cui all'art. 14 del Regolamento deve contenere: (i) l'indicazione delle categorie dei dati personali oggetto del trattamento; (ii) l'indicazione della fonte da cui hanno origine i dati personali, che può essere anche fonte accessibile al pubblico.

Rispetto all'informativa ex art. 13, non è necessario specificare la natura obbligatoria o meno del conferimento dei dati personali.

(iii) Data Breach[10] (Artt. 33 - 34)

Il GDPR prevede l'obbligo di **notificare le violazioni di dati personali** al Garante per la protezione dei dati personali entro 72 ore dal momento in cui se ne è venuti a conoscenza, a meno che sia improbabile che la suesposta violazione possa configurare un rischio per i diritti e le libertà degli interessati.

Tale notificazione quindi non deve essere sempre effettuata, in quanto il titolare è chiamato a valutare preventivamente la sussistenza di possibili rischi per i diritti e le libertà degli interessati.

Ove il titolare del trattamento dovesse ritenere che il rischio sia elevato, ne deve dare informazione, "*sempre senza giustificato ritardo*", anche agli interessati.

Tuttavia, come previsto dall'art. 34, par. 3, del GDPR, la comunicazione all'interessato non è richiesta in presenza di almeno una delle seguenti condizioni ovvero:

- l'adozione di misure tecniche e organizzative di protezione adeguate, ed applicazione delle stesse ai dati personali oggetto della violazione;
- la successiva adozione di misure atte a scongiurare il sopraggiungere di un rischio elevato per la tutela dei diritti e le libertà degli interessati;

[10] Si vedano, al riguardo le "Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679", adottate dal WP29 il 3 ottobre 2017, emendate in data 6 febbraio 2018 e reperibili al seguente link: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 .

- la comunicazione agli interessati richiederebbe sforzi non proporzionati. In tal caso gli interessati possono essere informati mediante una comunicazione pubblica o misura analoga.

Valutazione di impatto sulla protezione dei dati[11]

(artt. 35)

Il GDPR introduce il concetto di valutazione di impatto sulla protezione dei dati, che evidenzia la **responsabilizzazione** dei Titolari rispetto ai trattamenti da questi effettuati.

Tale valutazione consiste in un processo in cui è descritto il trattamento, nonché la correlata valutazione di necessità e di proporzionalità, nonché la **gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento** di dati personali.

La valutazione di impatto sulla protezione dei dati è richiesta quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono trattati dati sensibili, o anche per una combinazione di questi e altri fattori.

L'art. 35 par. 3 del GDPR prevede che la valutazione è obbligatoria nei casi in cui: a) sia necessaria "*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) sia necessario "*il trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9, par. 1 del GDPR, o di dati relativi a condanne penali e a reati di cui all'art. 10*"; c) sia prevista "*la sorveglianza sistematica su larga scala di una zona accessibile al pubblico*".

Possono sussistere, tuttavia, operazioni di trattamento a "rischio elevato" che non trovano collocazione in tale elenco ma che presentano rischi altrettanto elevati e pertanto soggetti alla valutazione di impatto sulla protezione dei dati.

[11] Si vedano, al riguardo le "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del Regolamento (UE) 2016/67", adottate dal WP29 il 4 aprile 2017, emendate in data 4 ottobre 2017 e reperibili al seguente link: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7015994

Sanzioni[12]

(artt. 83-84)

In un'ottica di rafforzamento della tutela dei diritti e delle libertà degli interessati, e di responsabilizzazione dei titolari e dei responsabili, il legislatore comunitario ha previsto un **inasprimento del regime sanzionatorio**.

In via esemplificativa:

- nel caso di violazione degli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli artt. 8 (Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione), 11 (Trattamento che non richiede l'identificazione), da 25 (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita) a 39 (Compiti del responsabile della protezione dei dati), 42 (Certificazione) e 43 (Organismi di certificazione) del GDPR, sono previste sanzioni amministrative pecuniarie fino a 10.000.000 euro, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore;
- nel caso di violazione dei principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli artt. 5, 6, 7 e 9 del GDPR, delle disposizioni sui diritti degli interessati a norma degli artt. da 12 a 22 del GDPR; delle disposizioni sul trasferimento di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli artt. da 44 a 49 del GDPR, sono previste sanzioni amministrative pecuniarie fino a 20.000.000 euro, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore

[12] Si vedano, al riguardo le "Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del Regolamento (UE) n. 2016/679", adottate dal WP29 il 3 ottobre 2017 e reperibili al seguente link: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7710776.

Appendice

Le linee guida del Garante della protezione dei dati personali in materia di Regolamento UE 2016/679

Il Garante della protezione dei dati ha adottato linee guida e altri documenti interpretativi in merito all'applicazione del GDPR, ossia:

- "**Linee guida sui responsabili della protezione dei dati**", adottate dal WP29 il 13 dicembre 2016, emendate in data 5 aprile 2017 (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5930287);
- "**Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679**", adottate dal WP29 il 4 aprile 2017, emendate in data 4 ottobre 2017 (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7015994);
- "**Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679**", adottate dal WP29 il 3 ottobre 2017, emendate in data 6 febbraio 2018 (http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052);
- "**Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del Regolamento (UE) n. 2016/679**", adottate dal WP29 il 3 ottobre 2017 (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7710776);
- "**Guida all´applicazione del Regolamento europeo in materia di protezione dei dati personali**" (https://www.garanteprivacy.it/documents/10160/0/Guida+all+applicazione+del+Regolamento+UE+2016+679.pdf).