Istituto per l'innovazione

Regolamento UE 2016/679

IL NUOVO REGOLAMENTO EUROPEO PRIVACY

Le principali novità per le Imprese

Autore: Cristiano Rigoli – Ufficio Legale & Compliance ICIE

Napoli, 19 gennaio 2017

PERIODO TRANSITORIO

• Il Parlamento Europeo, dopo oltre quattro anni di lavoro, con la Risoluzione Legislativa del 14 Aprile 2016, ha approvato in seduta plenaria il Regolamento Europeo Privacy relativo alla "Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati".

• Il nuovo Regolamento Europeo Privacy abroga la Direttiva 95/46/CE e mira a stabilire un'applicazione uniforme della normativa privacy in ogni Stato Membro dell'Unione Europea, garantendo in questo modo un maggior controllo da parte dei cittadini europei sui propri dati personali.

• Il 4 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il testo del Regolamento europeo in materia di protezione dei dati.

• Il Regolamento è vigente dal 24 maggio 2016, per diventare definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal **25 maggio 2018**. **Per tale data dovrà essere garantito il perfetto allineamento fra la normativa nazionale e le disposizioni del Regolamento.**

PERIODO TRANSITORIO

NOTA BENE

L'Art. 94 del Regolamento comma 1 recita:
"LA DIRETTIVA 95/46/CE è abrogata a decorrere dal 25 maggio 2018"

Fino al 25 maggio del 2018 rimane in vigore il d.lgs. 196/2003, si può applicare il nuovo regolamento 679/UE purché la norma non sia in contrasto con la normativa vigente

ESEMPIO Art. 18 della direttiva e art. 37 del d.lgs. 196/2003: obbligo di notificazione di alcuni trattamenti.

Nel nuovo Regolamento non c'è più la notificazione in termini generali come adempimento necessario per alcuni trattamenti.

Oggi e fino al 24 maggio 2018 si deve continuare a notificare i trattamenti (se si rientra nei casi previsti dall'art. 37 del codice privacy)

PERIODO TRANSITORIO

IL RAPPORTO TRA NORMATIVA EUROPEA E NORMATIVA NAZIONALE

In linea di principio la normativa di riferimento diviene il REGOLAMENTO 679/UE, la normativa italiana diviene residuale e potrà integrarlo.

A ben vedere il perimetro del Regolamento riguarda strettamente la parte che nell'attuale codice della privacy è quella generale: principi, diritti dell'interessato, informativa, consenso, ruoli, obblighi e sanzioni amministrative.

Non riguarda alcune specifiche aree, ancorché intersecate con la parte generale, che sono demandate alla normativa degli stati membri. Esempio:

- Libertà di espressione e di informazione
- Sanità pubblica
- Ricerca statistica
- Rapporti di lavoro e altro

PROVVEDIMENTI AUTORITA' GARANTE	→	Non decadano finché non saranno modificati, abrogati o sostituiti

PERIODO TRANSITORIO

LEGGE 25 ottobre 2017, n. 163: Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017.
(Gazzetta Ufficiale n. 259 del 6 novembre 2017)

In particolare l'**Art. 13** tratta della Delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) **2016/679**

Il Governo e' delegato ad adottare, entro sei mesi dalla data di entrata in vigore della presente legge, **uno o più decreti legislativi** al fine di **adeguare il quadro normativo nazionale** alle disposizioni del regolamento (UE) 2016/679

Comma 3. Nell'esercizio della delega di cui al comma 1 **il Governo e' tenuto a seguire**, anche i seguenti principi e criteri direttivi specifici:
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;
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.

PERIODO TRANSITORIO

Dopo aver delegato il Governo, il 25 ottobre, con legge 163/2017 a riorganizzare complessivamente il Codice Privacy per adeguarlo al GDPR (ed attuarne le disposizioni non direttamente applicabili), è poi intervenuto direttamente, il 20 novembre, con legge 167/2017 sul Codice Privacy (modificando l'art. 29 riguardante il *Responsabile del trattamento* ed introducendo l'art. 110 bis sul *Riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici*), successivamente con la cd. *legge anti-telemarketing* approvata il 22 dicembre 2017 e da ultimo con la legge di bilancio 205/2017.

Aspettiamo i decreti delegati di armonizzazione del Codice Privacy al GDPR. Non si può che sperare che facciano "piazza pulita" delle ultime disposizioni, creando un quadro normativo coerente e conforme alla normativa europea.

Legge 167 del 20 novembre 2017

Qui ci sono alcuni punti interessanti (e criticabili):

- l'**articolo 24** stabilisce che ora i dati di traffico telematico vanno conservati per 72 mesi (6 anni), mentre in precedenza la durata era di massimo 2 anni; *in tanti dicono che è follia; io non ho ancora capito se in questi anni questi dati sono serviti*;

- l'**articolo 28** allinea la nomina di responsabile del trattamento a quanto previsto dal GDPR, *sicuramente inutilmente (e senza una ragione apparente), visto che tra pochi mesi entrerà in vigore proprio il GDPR e quindi questa modifica non era proprio necessaria*;

- sempre l'articolo 28 prevede che il Garante pubblichi "schemi tipo" per stipulare accordi con i responsabili; *ad ora mi risulta siano disponibili solo quelli per il trasferimento dei dati extra-UE; mi pare un po' strano questo obbligo di usare "schemi tipo" (la formulazione del requisito non mi pare lasci margini di manovra); qualcuno ritiene che forse questo è per evitare che i contratti stipulati oggi con la PA siano messi in discussione a maggio;*

- sempre l'articolo 28 impone restrizioni nel riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici; *ci sono un paio di questioni bizzarre: la richiesta di autorizzazione preventiva al Garante, nonostante il GDPR, volontariamente, non la preveda più, e l'introduzione del silenzio-rigetto (ulteriore aberrazione);*

- l'articolo 29 stanzia maggiori fondi al Garante e permette l'aumento di organico (*mi viene da pensare che prevedono maggiori introiti grazie alle nuove sanzioni amministrative*).

PERIODO TRANSITORIO

Legge 205 del 22 dicembre 2017

Forse quest'ultimo intervento, se possibile, suscita ancor più perplessità dei precedenti, oltre che per i termini utilizzati (fra cui, "*informativa*" per la comunicazione/notifica al Garante, "*titolare dei dati*" per titolare del trattamento), per la sua palese incompatibilità con il GDPR.

Il nostro legislatore ha infatti reintrodotto la "***notifica***" al Garante - eliminata dal legislatore europeo in quanto ritenuta un mero onere amministrativo e finanziario che non ha contribuito a migliorare la protezione dei dati - nel caso in cui il titolare "*effettui un trattamento fondato sull'**interesse legittimo** che prevede **l'uso di nuove tecnologie** o di strumenti automatizzati*". È stato infatti previsto che, in tale ipotesi, il "*titolare di dati personali*" (!) deve "*darne tempestiva comunicazione al Garante*", inviando un'"*informativa*" (!) relativa all'oggetto, alle finalità e al contesto del trattamento, utilizzando il modello che dovrà essere predisposto dal Garante entro due mesi dall'entrata in vigore della legge. Trascorsi quindici giorni lavorativi, in assenza di risposta, il titolare può procedere al trattamento, ma il Garante potrà comunque sospenderlo (per un massimo di 30 giorni) per chiedere "*ulteriori informazioni e integrazioni*" o **disporne l'inibitoria** "*qualora ritenga che dal trattamento derivi comunque **una lesione dei diritti e delle libertà del soggetto interessato***".

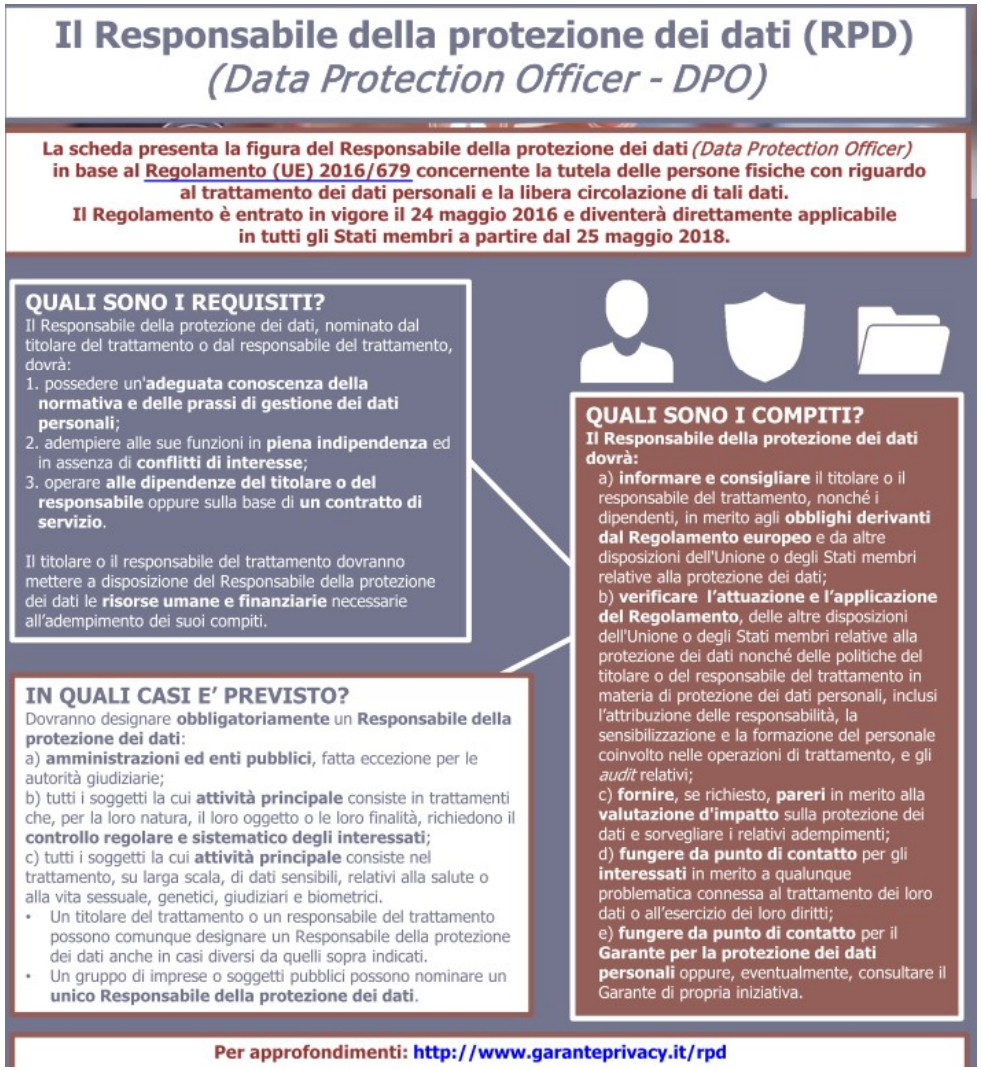
Tali disposizioni appaiono manifestamente incompatibili con il GDPR in virtù del quale, nel caso in cui "*un tipo di trattamento, allorché prevede in particolare **l'uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**»,* è il Titolare, in autonomia, a dover effettuare una *valutazione (preminare) d'impatto* del trattamento stesso sulla protezione dei dati (la c.d. **DPIA**). L'obbligo di consultazione al Garante è residuale, per le sole ipotesi in cui dalla valutazione d'impatto risulta che il trattamento presenterebbe comunque un rischio elevato che non può essere attenuato con «*misure opportune in termini di tecnologia disponibile e costi di attuazione*» .

PRINCIPALI NOVITA'

- **La nomina del DPO – DATA PROTECTION OFFICER**
- **Il principio di accountability**
- **La valutazione di impatto**
- **L'adozione delle misure tecniche e organizzative ADEGUATE**
- **Il registro delle attività di trattamento**
- **La notificazione della violazione dei dati (c.d. data breach)**
- **I nuovi diritti dell'interessato**
- **I codici di condotta e le certificazioni**

ISTITUTO COOPERATIVO PER L'INNOVAZIONE

PRINCIPALI NOVITA'



PRINCIPALI NOVITA'

Approccio basato sul rischio e misure di accountability di titolari e responsabili

Il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull' adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento).

Non ci sono più misure minime, ma solo misure di sicurezza adeguate

Il nuovo Regolamento Europeo sulla privacy non definisce misure minime di sicurezza, come avviene per l'attuale normativa italiana sulla privacy (c.d. Allegato B al d.lgs. 196/2003), ma sposta la responsabilità di definire le misure di sicurezza idonee a garantire la privacy dei dati personali trattati sul titolare o responsabile del trattamento, dopo un'attenta analisi dei rischi.

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

PRINCIPALI NOVITA'

Il primo fra tali criteri è sintetizzato dall'espressione inglese "**data protection by default and by design**" (si veda art. 25), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25, paragrafo 1 del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

PRINCIPALI NOVITA’

Valutazione di impatto sulla protezione dei dati (Art. 35 GDPR)

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.

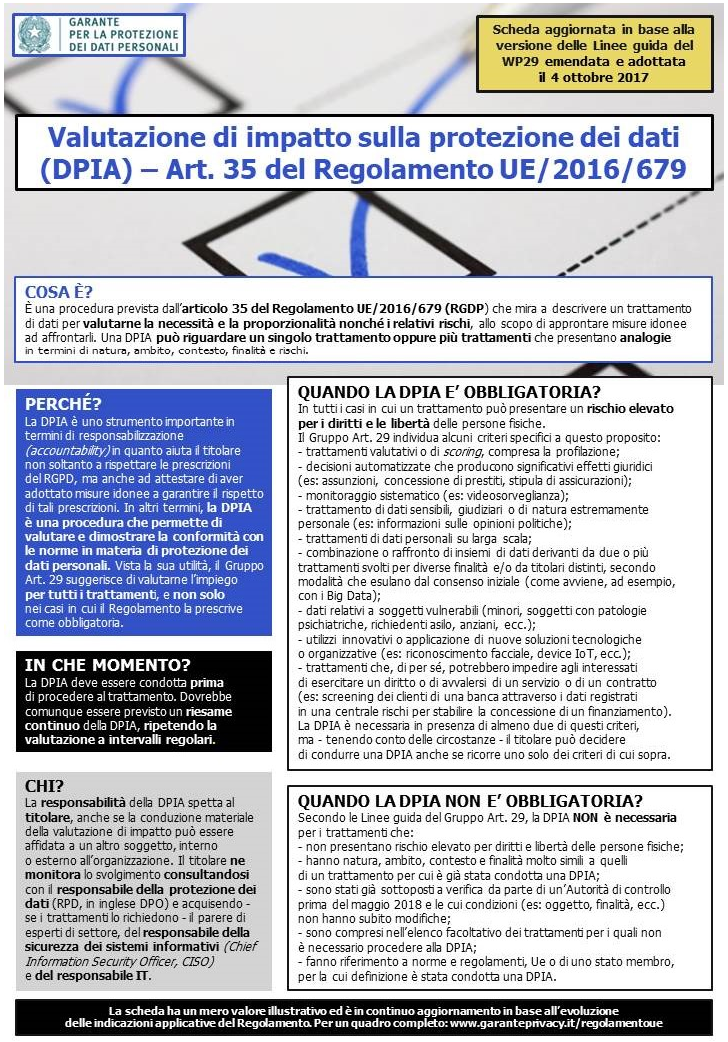
La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

- trattamenti automatizzati di profilazione sistematica
- trattamento, su larga scala, di dati sensibili o giudiziari
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico

Il Garante redigerà un elenco delle tipologie di trattamenti soggetti a privacy impact assessment.

ISTITUTO COOPERATIVO PER L'INNOVAZIONE

PRINCIPALI NOVITA'



GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Scheda aggiornata in base alla versione delle Linee guida del WP29 emendata e adottata il 4 ottobre 2017

Valutazione di impatto sulla protezione dei dati (DPIA) – Art. 35 del Regolamento UE/2016/679

COSA È?

È una procedura prevista dall'**articolo 35 del Regolamento UE/2016/679 (RGDP)** che mira a descrivere un trattamento di dati per **valutarne la necessità e la proporzionalità nonché i relativi rischi**, allo scopo di approntare misure idonee ad affrontarli. Una DPIA **può riguardare un singolo trattamento oppure più trattamenti** che presentano **analogie** in termini di natura, ambito, contesto, finalità e rischi.

PERCHÉ?

La DPIA è uno strumento importante in termini di responsabilizzazione *(accountability)* in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, **la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali.** Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego **per tutti i trattamenti**, e **non solo** nei casi in cui il Regolamento la prescrive come obbligatoria.

IN CHE MOMENTO?

La DPIA deve essere condotta **prima** di procedere al trattamento. Dovrebbe comunque essere previsto un **riesame continuo** della DPIA, **ripetendo la valutazione a intervalli regolari.**

CHI?

La **responsabilità** della DPIA spetta al **titolare**, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare **ne monitora** lo svolgimento **consultandosi** con il **responsabile della protezione dei dati** (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del **responsabile della sicurezza dei sistemi informativi** *(Chief Information Security Officer, CISO)* e **del responsabile IT.**

QUANDO LA DPIA E' OBBLIGATORIA?

In tutti i casi in cui un trattamento può presentare un **rischio elevato per i diritti e le libertà** delle persone fisiche.
Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:
- trattamenti valutativi o di *scoring*, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

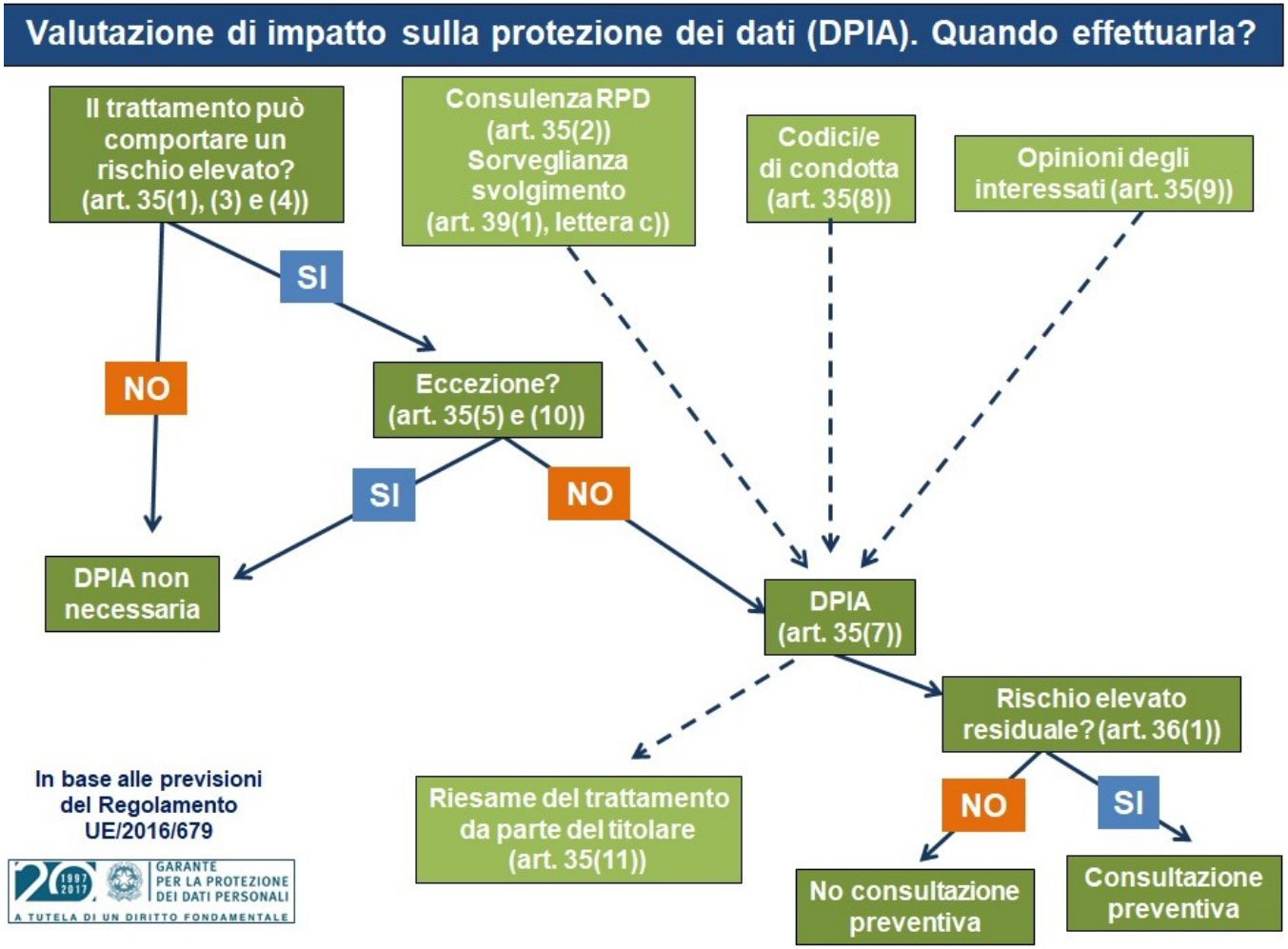
QUANDO LA DPIA NON E' OBBLIGATORIA?

Secondo le Linee guida del Gruppo Art. 29, la DPIA **NON è necessaria** per i trattamenti che:
- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento. Per un quadro completo: www.garanteprivacy.it/regolamentoue

ISTITUTO COOPERATIVO PER L'INNOVAZIONE

PRINCIPALI NOVITA'



PRINCIPALI NOVITA’

Registro delle attività di trattamento (art. 30 GDPR)

Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.

Tale adempimento **non si applica 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 dati sensibili o giudiziari

PRINCIPALI NOVITA'

Notificazione di una violazione dei dati personali alla autorità di controllo (Art. 33 GDPR) c.d. data breach

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.

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.

ISTITUTO COOPERATIVO PER L'INNOVAZIONE

PRINCIPALI NOVITA'

DATA BREACH: gli obblighi nella normativa italiana attuale

SOCIETA' TELEFONICHE E INTERNET PROVIDER

Art. 32-*bis* del Codice in materia di protezione dei dati personali (d. lgs. 196/2003), Regolamento UE 611/13, Provvedimento del Garante n. 161 del 4 aprile 2013 [doc. web n. 2388260]

- L'obbligo di comunicazione al Garante *(mediante un apposito modello di comunicazione)* riguarda i fornitori di servizi telefonici e di accesso a Internet (e non, ad esempio, i siti internet che diffondono contenuti, i motori di ricerca, gli *internet point*, le reti aziendali).
- In caso di violazione dei dati personali, società di tlc e Isp devono:
  a. entro 24 ore dalla scoperta dell'evento, fornire al Garante le informazioni necessarie a consentire una prima valutazione dell'entità della violazione
  b. entro 3 giorni dalla scoperta, informare anche ciascun utente coinvolto, comunicando gli elementi previsti dal Regolamento 611/2013 e dal provvedimento del Garante n. 161 del 4 aprile 2013.
- La comunicazione agli utenti non è dovuta se si dimostra di aver utilizzato misure di sicurezza nonché sistemi di cifratura e di anonimizzazione che rendono inintelligibili i dati. Nei casi più gravi, il Garante può comunque imporre la comunicazione agli interessati.
- Per consentire l'attività di accertamento del Garante, società telefoniche e provider devono tenere un inventario costantemente aggiornato delle violazioni subite.
- **SANZIONI AMMINISTRATIVE PREVISTE (art. 162-*ter* del Codice in materia di protezione dei dati personali)**
  - per mancata o ritardata comunicazione al Garante: da 25mila a 150mila euro;
  - per omessa o mancata comunicazione agli utenti: da 150 euro a 1000 euro per ogni società, ente o persona interessata;
  - per mancata tenuta dell'inventario delle violazioni aggiornato: da 20mila a 120mila euro.

BIOMETRIA

Provvedimento n. 513 del 12 novembre 2014 [doc. web n. 3556992]

- Entro 24 ore dalla conoscenza del fatto, i titolari del trattamento (aziende, amministrazioni pubbliche, ecc.) comunicano al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.

DOSSIER SANITARIO ELETTRONICO

Provvedimento n. 331 del 4 giugno 2015 [doc. web n. 4084632]

- Entro 48 ore dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.

AMMINISTRAZIONI PUBBLICHE

Provvedimento n. 392 del 2 luglio 2015 [doc. web n. 4129029]

- Entro 48 ore dalla conoscenza del fatto, le amministrazioni pubbliche sono tenute a comunicare al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati.

PRINCIPALI NOVITA’

Diritto alla portabilità dei dati (art. 20 GDPR)

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell’interessato o sulla base di un contratto stipulato con l’interessato (quindi non si applica ai dati il cui trattamento si fonda sull’interesse pubblico o sull’interesse legittimo del titolare, per esempio), e solo i dati che siano stati “forniti” dall’interessato al titolare.

Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall’interessato, se tecnicamente possibile.

ISTITUTO COOPERATIVO PER L'INNOVAZIONE

PRINCIPALI NOVITA'

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Scheda aggiornata in base alla versione delle Linee guida del WP29 emendata e adottata il 5 aprile 2017

Il diritto alla portabilità dei dati

La scheda presenta il diritto alla portabilità dai dati in relazione a quanto previsto dal Regolamento (UE) 2016/679 e dalle Linee-guida del WP29

COSA È?
È un diritto innovativo previsto dall'articolo 20 del regolamento (Ue) 2016/679 che consente all'interessato **di ricevere i dati personali forniti a un titolare**, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di **trasmetterli a un altro titolare** del trattamento senza impedimenti.

QUALI VANTAGGI PUO' OFFRIRE?
- **facilitare il passaggi**o da un fornitore di servizi all'altro;
- consentire la **creazione di nuovi servizi** nel quadro della strategia dell'Ue per il mercato unico digitale;
- offrire la possibilità di «**riequilibrare**» **il rapporto fra interessati e titolari del trattamento** tramite l'affermazione dei diritti e del controllo spettanti agli interessati in rapporto ai dati personali che li riguardano.

COSA PERMETTE DI FARE?
- **ricevere dati personali** trattati da un titolare e conservarli su un supporto personale o un *cloud* privato in vista di un utilizzo ulteriore per scopi personali, senza trasmetterli necessariamente a un altro titolare *(es: recuperare l'elenco dei brani musicali preferiti detenuto da un servizio di musica in streaming, per scoprire quante volte si sono ascoltati determinati brani);*
- **trasmettere dati personali** da un titolare del trattamento a un altro titolare del trattamento *(es.: un diverso fornitore di servizi).*

L'esercizio del diritto alla portabilità dei dati **non pregiudica nessuno degli altri diritti** dell'interessato, che può, per esempio:
- **continuare a fruire del servizio** offerto dal titolare anche dopo un'operazione di portabilità;
- **esercitare il diritto di cancellazione** *(o «diritto all'oblio»)* ai sensi dell'art. 17 del regolamento.

QUANDO TROVA APPLICAZIONE?
Per essere portabili i dati devono:
- essere **dati personali chiaramente riferibili all'interessato**. Sono quindi ad esempio esclusi i dati anonimi;
- essere **trattati sulla base del consenso preventivo** dell'interessato o di un **contratto** di cui è parte l'interessato;
- essere **trattati attraverso strumenti automatizzati**. Sono quindi esclusi gli archivi e registri cartacei;
- essere stati **forniti consapevolmente** e in modo attivo dall'interessato *(ad es., i dati di registrazione inseriti compilando un modulo online, come indirizzo postale, nome utente, età, ecc.).*
- Sono compresi anche i **dati osservati forniti dall'interessato attraverso la fruizione di un servizio o l'utilizzo di un dispositivo** *(es.: la cronologia delle ricerche effettuate dall'interessato, i dati relativi al traffico, i dati relativi all'ubicazione, dati grezzi come la frequenza cardiaca registrata da dispositivi sanitari o di fitness.)*

Il diritto alla portabilità **non si applica** invece ai «dati inferenziali» né ai «dati derivati» *(es.: l'esito di una valutazione concernente la salute di un utente o il profilo creato al fine di attribuire uno score creditizio o di ottemperare a normativa antiriciclaggio).*

L'esercizio del diritto alla portabilità **non deve ledere i diritti e le libertà altrui**.

I dati portabili **devono essere forniti in un formato «interoperabile»**, ossia in un formato che ne consenta il riutilizzo. I titolari potranno utilizzare formati di impiego comune, se già esistenti, oppure utilizzare formati aperti (es. XML), ovvero sviluppare formati interoperabili e strumenti informatici che consentano di estrarre i dati pertinenti.

La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento.
Per un quadro completo si invita a consultare la pagina www.garanteprivacy.it/portabilita

PRINCIPALI NOVITA'

Diritto di cancellazione (art.17 GDPR)

Il diritto cosiddetto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2).

Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (si veda art. 17, paragrafo 1).

PRINCIPALI NOVITA'

Codici di condotta (Art. 40 GDPR)

Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento possono elaborare codici di condotta.

I codici di condotta possono essere approvati dalla autorità di controllo che ne certifica la conformità al regolamento.

La commissione europea può decidere che i codici di condotta approvati hanno validità generale all'interno dell'unione.

PRINCIPALI NOVITA'

Certificazione (Art. 42 GDPR)

Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese.

La certificazione viene rilasciata da organismi accreditati dalla autorità di controllo o dall'organismo nazionale di accreditamento.

La certificazione garantisce la conformità del trattamento e delle misure di scurezza al regolamento.

La certificazione viene rilasciata per un periodo massimo di 3 anni – rinnovabili - e può essere revocata se vengono meno i requisiti. L'ente di certificazione deve comunicare alla autorità di controllo i motivi di rilascio o revoca.

SANZIONI

LE SANZIONI (Art. 83 GDPR)

Il nuovo Regolamento ha notevolmente innalzato l'ammontare delle sanzioni amministrative pecuniarie previste per la violazione della normativa privacy (sanzioni che potranno arrivare fino ad un massimo di 20 milioni di Euro o fino al 4% del fatturato mondiale totale annuo), lasciando poi a ciascuno Stato membro la facoltà di adottare, entro il 25 maggio 2018, altre sanzioni – effettive, proporzionate e dissuasive – per le violazioni del Regolamento.

Le sanzioni penali rimangono di competenza di ogni singolo Stato.

COSA FARE?

Come gestire al meglio l'adeguamento della propria cooperativa

1. CONOSCERE I PRINCIPI DEL NUOVO REGOLAMENTO

2. VALUTARE LE SOLUZIONI DA ADOTTARE PER RENDERE CONFORMI I SISTEMI AZIENDALI

3. COGLIERE L'OPPORTUNITA' DEL CAMBIAMENTO AL FINE DI MIGLIORARE LA GESTIONE DELLA SICUREZZA:
   - ✓ Monitorare gli accessi al patrimonio dati
   - ✓ Rilevare utilizzi anomali
   - ✓ Controllare QUALI dati sono accessibili a CHI

COSA FARE?

COSA POSSIAMO FARE DA OGGI AL 24 MAGGIO 2018…

1. Consapevolezza e formazione: accertarsi che le persone chiave delle struttura organizzativa del Titolare siano consapevoli dell'impatto che avrà il Regolamento, mappare le aree di rischio, individuare quelle che saranno maggiormente interessate dai cambiamenti e i ruoli decisionali. Organizzare delle sessioni formative per i ruoli apicali della azienda/ente.
2. Fare un nuovo censimento di tutti i trattamenti: documentare i dati personali trattati, individuare la base giuridica, verificare la durata della conservazione dei dati e a chi vengo comunicati...
3. Analizzare i rischi che gravano sui trattamenti e predisporre le misure «adeguate»
4. Per i trattamenti che presentano un rischio elevato per i diritti e libertà delle persone fisiche effettuare la valutazione di impatto (PIA)
5. Redigere il registro delle attività di trattamento
6. Rivedere tutte le informative e aggiornare il contenuto sulla base del nuovo art. 13.
7. Nominare il Responsabile della protezione dati (se obbligati) o valutare la sua designazione come misura adeguata
8. Aggiornare le designazioni dei responsabili