Stato: maggio 2018

Il GDPR e le sue conseguenze per la Svizzera[1]

Contenuto

[1] *Attenzione: il presente testo sarà completato e modificato in base all'evoluzione della riflessione a livello nazionale ed europeo. Infatti, sono in corso chiarimenti per conoscere la posizione e l'interpretazione delle autorità di riferimento e di controllo (G29, Commissione europea, autorità di controllo degli Stati membri dell'Unione).*

Introduzione: revisione del quadro giuridico europeo in materia di protezione dei dati

Nel gennaio 2012 la Commissione europea ha proposto una serie di misure legislative allo scopo di aggiornare e attualizzare le norme contenute nella direttiva del 1995 sulla protezione dei dati (direttiva 95/46/CE) e nella decisione quadro del 2008 sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (decisione quadro 2008/977/GAI). Questa riforma è volta a creare un insieme di norme uniformi all'interno dell'UE adattate all'era digitale, a migliorare la certezza del diritto e a rafforzare la fiducia dei cittadini e delle imprese nel mercato unico del digitale. La riforma include una comunicazione con cui la Commissione espone i suoi obiettivi e due proposte legislative: un regolamento generale sulla protezione dei dati e una direttiva specifica per il settore relativo alla polizia e alla giustizia.

Il 14 aprile 2016, con l'approvazione dei testi proposti, il Parlamento europeo ha concluso oltre quattro anni di lavori. Le norme contenute nel regolamento generale sulla protezione dei dati saranno direttamente applicabili in tutti gli Stati membri a partire dal 25 maggio 2018. I Paesi dell'UE avranno tempo fino al 6 maggio 2018 per recepire le disposizioni della direttiva nelle rispettive legislazioni nazionali.

Il regolamento generale sulla protezione dei dati (GDPR)

Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati o GDPR) è stato approvato dal Parlamento europeo il 14 aprile 2016 ed entrerà in vigore il **25 maggio 2018**. A partire da quella data, il GDPR sarà direttamente applicabile a tutti gli attori attivi sul territorio dell'Unione europea. Infatti, nel diritto dell'Unione europea, tutti gli elementi di un regolamento sono obbligatori a partire dall'entrata in vigore (non possono quindi essere applicati in modo selettivo). Contrariamente alla direttiva, il regolamento è direttamente applicabile in tutta l'Unione europea senza bisogno di essere recepito nelle varie legislazioni degli Stati membri. Le nuove norme conferiscono ai cittadini più controllo sui loro dati personali, responsabilizzano maggiormente le imprese riducendo nel contempo i loro oneri dichiarativi e rafforzano il ruolo delle autorità di protezione dei dati. **Questo testo di riferimento per l'Europa avrà ripercussioni dirette su numerose imprese svizzere**.

Ambito di applicazione materiale (art. 2 GDPR)

Rispetto alla direttiva 95/46/CE, non vi sono stati cambiamenti di principio per quanto riguarda l'ambito di applicazione materiale. Il GDPR si applica *«al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi»* (art. 2 § 1 GDPR). Esso concerne tutti i dati personali che si riferiscono a persone fisiche identificate o identificabili e non distingue fra trattamento effettuato da una persona fisica o giuridica di diritto pubblico o privato. L'articolo 2 paragrafo 2 GDPR prevede quattro eccezioni; il GDPR «non si applica ai trattamenti di dati personali*:*

> *a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;*
> *b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;*
> *c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;*

d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.»

Il GDPR riguarda il trattamento dei dati personali relativi alle persone fisiche, indipendentemente dalle nazionalità o residenza. Ciò significa che i dati personali di una persona fisica domiciliata in Svizzera che sono trattati in uno Stato membro dell'Unione europea rientrano nel campo d'applicazione del GDPR.

Ambito di applicazione territoriale (art. 3 GDPR)

Rispetto alla direttiva 95/46/CE, l'ambito di applicazione è stato esteso e ora contempla il criterio dell'individuazione del pubblico oggetto del trattamento dei dati (applicazione extraterritoriale). Fra l'altro, quest'estensione è conforme alla giurisprudenza della Corte di giustizia dell'Unione europea (CGUE) che, nel 2014, si era pronunciata a favore dell'applicazione extraterritoriale della direttiva nella causa Google Spain e Google (C-131-12).

L'articolo 3 GDPR stabilisce quanto segue:

1. *Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.*
2. *Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:*
   a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; ***oppure***
   b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.
3. *Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.*

L'applicazione del GDPR dipende dunque dai due criteri di collegamento seguenti:

1. **Il criterio dello stabilimento** (= luogo di stabilimento del titolare del trattamento o di un responsabile del trattamento; art. 3 § 1): il titolare del trattamento o il responsabile del trattamento è stabilito **nell'Unione europea**. In questo caso il regolamento si applica d'ufficio indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione. Nella causa Weltimmo c. NAIH (C-230/14), la CGUE ha interpretato la nozione di stabilimento in modo relativamente ampio e flessibile.

2. **Il criterio di individuazione** (= il luogo in cui si trovano gli interessati dal trattamento; art. 3 § 2): il titolare del trattamento è stabilito **al di fuori** dell'Unione europea ma le sue attività di trattamento riguardano sia l'offerta di beni o servizi a interessati che si trovano sul territorio dell'Unione, sia il monitoraggio del comportamento di tali interessati se tale

comportamento ha luogo all'interno dell'Unione. In quest'ultimo caso di monitoraggio, il legislatore europeo si riferisce in primo luogo al monitoraggio degli internauti. In pratica il GDPR dovrebbe applicarsi qualora un residente europeo, indipendentemente dalla sua nazionalità o dal suo domicilio, sia direttamente oggetto di un trattamento dei dati.

Nel valutare l'applicabilità del regolamento, occorrerà sempre tener conto del singolo caso e in particolare dell'intenzione del titolare del trattamento di offrire beni o servizi a persone che si trovano sul territorio dell'Unione oppure di monitorare il comportamento di queste ultime.

Diritti degli interessati

Uno degli obiettivi della riforma europea è attribuire **maggiore controllo e visibilità** agli interessati. L'articolo 12 GDPR obbliga il titolare del trattamento a prevedere procedure e meccanismi che consentano all'interessato di esercitare i propri diritti. Stabilisce il principio della trasparenza: le informazioni destinate al pubblico o all'interessato devono essere facilmente accessibili e di facile comprensione, formulate in modo conciso e trasparente con un linguaggio semplice e chiaro – in particolar modo nel caso di informazioni destinate ai minori. Di norma, le informazioni saranno fornite per scritto e gratuitamente. Il regolamento prevede anche un termine entro il quale tali informazioni dovranno essere fornite. Tutte le modalità di cui all'articolo 12 GDPR sono applicabili a tutti i diritti previsti dal regolamento, ossia:

- **Il diritto all'informazione** (articoli 13 e 14 GDPR)
  In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, tutta una serie d'informazioni. Il titolare del trattamento fornisce all'interessato delle informazioni anche qualora i dati non siano stati ottenuti presso l'interessato stesso.

- **Il diritto di accesso** (articolo 15 GDPR)
  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 come pure alle informazioni complementari previste alle lettere a) – h). Questo diritto comprende anche quello di ottenere una copia dei dati personali oggetto di trattamento.

- **Il diritto di rettifica** (articolo 16 GDPR)
  L'interessato ha il diritto di chiedere la rettifica o l'integrazione dei suoi dati personali incompleti senza ingiustificato ritardo.

- **Il diritto alla cancellazione («diritto all'oblio»)** (articolo 17 GDPR)
  L'interessato ha il diritto di chiedere la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, se sussiste uno dei motivi di cui al paragrafo 1. Se i dati personali dell'interessato sono stati trasmessi ad altre entità, s'innesca il meccanismo del «diritto all'oblio»: il titolare del trattamento dovrà adottare tutte le misure ragionevoli per informare le altre entità della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

- **Il diritto di limitazione di trattamento** (articolo 18 GDPR)
  In alcuni casi previsti dalla legge l'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione di trattamento dei suoi dati personali. Se viene richiesta tale limitazione, il titolare del trattamento potrà soltanto conservare i dati personali. Di norma, non potrà più essere effettuata alcuna operazione su questi dati personali.

- **L'obbligo di notifica da parte del titolare** (articolo 19 GDPR)
  Quest'articolo istituisce un obbligo di notifica che incombe al titolare del trattamento, il quale è tenuto a comunicare a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento.

- **Il diritto alla portabilità dei dati** (articolo 20 GDPR)
  L'interessato ha il diritto di recuperare in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento, per esempio per poter cambiare fornitore di servizi. Questo diritto può essere utilizzato unicamente qualora il trattamento dei dati si basi sul consenso dell'interessato o su un contratto.

- **Il diritto di opposizione** (articolo 21 GDPR)
  L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano effettuato per l'interesse pubblico o il legittimo interesse del titolare del trattamento, compresa la profilazione effettuata in base alle disposizioni relative all'interesse pubblico o al legittimo interesse. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di un interesse preponderante o di una legge specifica. L'interessato ha pure il diritto di opporsi al trattamento dei dati personali che lo riguardano per finalità di marketing diretto.

- **Il diritto a non essere sottoposto a processo decisionale automatizzato** (articolo 22 GDPR)
  L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. La profilazione vi è espressamente inclusa.

- **Il diritto alla comunicazione di una violazione dei dati personali** (articolo 34 GDPR).
  Il titolare del trattamento è tenuto a comunicare all'interessato le violazioni dei dati personali suscettibili di presentare un rischio elevato per i suoi diritti e le sue libertà.

Il regolamento prevede inoltre una protezione specifica per i minori, dato che sono meno consapevoli dei rischi, delle conseguenze e dei loro diritti in relazione alla protezione dei dati. L'articolo 8 GDPR prevede che qualora servizi della società dell'informazione siano direttamente offerti ai minori, il consenso al trattamento dei dati del minore deve essere prestato o autorizzato dal titolare della responsabilità genitoriale del minore (gli Stati membri sono liberi di fissare l'età limite tra i 13 e i 16 anni).

Applicabilità alle imprese svizzere (art. 3 e 27 GDPR)

Dal testo del regolamento e dai suoi considerandi risulta che il GDPR sarà applicabile alle imprese svizzere nei casi previsti dal criterio:

Dello stabilimento (art. 3 § 1; cons. 22):

trattamento di dati personali effettuato nell'ambito delle attività di una succursale o filiale dotata di personalità giuridica[2] europea di un'impresa svizzera sul territorio dell'Unione;

Un responsabile del trattamento sul territorio dell'Unione (ad es. un fornitore di servizi informatici) che tratta dati personali per un'impresa svizzera è soggetto al GDPR indipendentemente dal fatto che tratti dati di interessati che si trovano in Svizzera o nell'Unione (art. 3 § 1). È tenuto a rispettare gli obblighi specifici dei responsabili del trattamento stabiliti dal GDPR (cfr. articoli 28, 30 § 2 e 37 GDPR) e i requisiti derivanti dal diritto svizzero (cfr. articolo 10*a* LPD). In caso di non conformità è probabile che se ne assuma la responsabilità. Ciò non significa tuttavia che il titolare del trattamento in Svizzera sia soggetto al regolamento.

Dell'individuazione (art. 3 § 2; cons. 23 e 24):

- trattamento di dati personali di interessati che si trovano nell'Unione effettuato da un'impresa stabilita in Svizzera per **l'offerta di beni o la prestazione di servizi** a interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato (art. 3 § 2 (a) GDPR);

Esempio 1: un'impresa stabilita in Svizzera vende orologi a persone domiciliate in Francia, Belgio, Portogallo, Finlandia e Grecia mediante un negozio on line. Il GDPR è applicabile perché la società svizzera offre beni a persone che si trovano nell'Unione.

Il GDPR non dà una definizione precisa delle nozioni di offerta di beni e prestazione di servizi. Il considerando 23 indica che occorre stabilire *«se risulta che il titolare o il responsabile del trattamento intenda fornire servizi agli interessati in uno o più Stati membri dell'Unione».* Per stabilire quest'intenzione, è necessario prendere in considerazione una serie d'indizi tra i quali figurano per esempio: *«l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, la possibilità di ordinare beni e servizi in tale altra lingua, la menzione di clienti o utenti che si trovano nell'Unione»*.

In un altro contesto (cfr. Cause riunite C-585/08 e C-144/09), la CGUE ha già valutato se l'offerta di beni e di servizi potesse essere considerata come diretta verso lo Stato membro dell'Unione. Al riguardo, ha inoltre rilevato i seguenti fattori: la menzione di un numero di telefono con un prefisso internazionale, la descrizione dell'itinerario da uno Stato membro al luogo in cui il servizio è offerto (p. es. un albergo svizzero che indica l'itinerario per raggiungerlo dall'estero), la menzione sul sito web di una clientela internazionale domiciliata in vari Stati membri dell'Unione, l'utilizzo di un dominio Internet di primo livello diverso da quello dello

[2] Il considerando 22 del GDPR precisa che lo stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. A tale riguardo, non è determinante la forma giuridica assunta.

Stato membro in cui è offerto il servizio (p. es. il sito www.exemple.ch è accessibile anche con www.exemple.fr e www.exemple.eu).

Tuttavia, *«la semplice accessibilità del sito web del titolare del trattamento, del responsabile del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica o di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il titolare del trattamento è stabilito sono insufficienti per accertare tale intenzione»*.

Occorre ciononostante sottolineare che l'elenco di fattori citati non è esauriente e che la questione dovrà sempre essere analizzata caso per caso.

trattamento su commissione: trattamento di dati personali effettuato da un'impresa svizzera[3] in qualità di responsabile del trattamento per conto di un'impresa europea.

- trattamento di dati personali di residenti dell'Unione effettuato da un'impresa stabilita in Svizzera per il **monitoraggio del comportamento** che tali interessati hanno all'interno dell'Unione (art. 3 § 2 (b) GDPR).

  Per quanto riguarda la nozione di monitoraggio e la definizione di che cosa possa essere considerato come un'attività di trattamento, il considerando 24 indica che *«è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali»*.

  Si tratterà in particolare della pubblicità comportamentale che, come la definisce il gruppo di lavoro dell'articolo 29 nel suo parere sulla pubblicità comportamentale, *«si basa sull'osservazione del comportamento delle persone nel tempo. Questo tipo di pubblicità cerca di studiare le caratteristiche del comportamento delle persone attraverso le loro azioni (frequentazione ripetuta di certi siti, interazioni, parole chiave, produzione di contenuti online, ecc.) al fine di elaborare un profilo specifico e quindi inviare messaggi pubblicitari che corrispondano perfettamente agli interessi dedotti»*.

  Esempio 2: un albergatore della Valle Leventina crea dei profili dei suoi clienti italiani, svedesi, tedeschi e polacchi per proporre loro delle offerte per altri soggiorni; il GDPR è applicabile se il profilo è creato in base al comportamento all'interno dell'UE.

  Esempio 3: il gestore di un sito web che ricorre al web tracking per seguire le attività dei suoi visitatori o per osservare il loro comportamento di navigazione potrà risalire agli interessi, alle preferenze o alle abitudini degli internauti. Il GDPR è dunque senz'altro applicabile.

[3] A condizione che la società svizzera intenda offrire beni e servizi a residenti dell'Unione europea.

Obblighi delle imprese assoggettate al regolamento

Una delle maggiori novità rispetto alla direttiva 95/46/CE è la consacrazione del principio di responsabilità («*accountability*») del titolare del trattamento (cfr. art. 5 § 2 GDPR) in virtù del quale il titolare del trattamento è **attivamente responsabile** che il trattamento dei dati personali avvenga conformemente al regolamento. Il titolare del trattamento è responsabile del rispetto dei principi generali e deve essere anche in grado di comprovare tale conformità. È in base a questo principio che si è giunti al principio dell'**inversione dell'onere della prova**. Il regolamento prevede in particolare i seguenti obblighi:

- l'articolo 24 GDPR sottolinea che il principio di responsabilità va di pari passo con l'approccio basato sul rischio, secondo cui il titolare del trattamento deve valutare in modo obiettivo la probabilità e la gravità del rischio che i diritti e le libertà delle persone fisiche corrono a seguito del suo trattamento. Il titolare del trattamento dovrà dunque mettere in atto meccanismi e sistemi di controllo in seno alla sua organizzazione per garantire che il trattamento rimanga conforme durante tutta la sua durata e per conservarne la prova;

- l'articolo 25 GDPR introduce i principi della **protezione dei dati fin dalla progettazione e della protezione per impostazione predefinita**. Tali principi impongono che fin dalla fase di progettazione dei prodotti e dei servizi si prevedano garanzie in materia di protezione dei dati;

- l'articolo 30 GDPR prevede che ogni titolare del trattamento o il suo rappresentante tenga un **registro delle attività di trattamento** (in formato elettronico) svolte sotto la sua responsabilità. L'articolo 30 paragrafo 1 GDPR specifica il contenuto del registro. Questo registro dovrà, su richiesta, essere messo a disposizione dell'autorità di protezione dei dati. Salvo eccezioni, le imprese con meno di 250 dipendenti non sottostanno a tale obbligo (cfr. art. 30 § 5 GDPR);

- l'articolo 35 GDPR prevede lo svolgimento di una **valutazione dell'impatto** sulla protezione dei dati nei casi in cui un trattamento possa presentare un rischio elevato per i diritti e le libertà degli interessati[4]. Se quest'analisi preliminare evidenzia rischi particolari, il titolare del trattamento dovrà consultare l'autorità di controllo indipendente prima di iniziare il trattamento; se è stato designato un responsabile della protezione dei dati, il titolare del trattamento dovrà consultarlo. In alcuni casi specifici la valutazione d'impatto sarà obbligatoria (cfr. art. 35 § 3); il suo contenuto minimo è descritto nell'articolo 35 paragrafo 7.

La **sicurezza dei trattamenti** è diventata un principio basilare della protezione dei dati nel regolamento:

- l'articolo 32 GDPR obbliga il titolare del trattamento a mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio. Nel fare ciò, deve tener conto dello stato dell'arte e dei costi di attuazione, nonché della natura,

[4] Per aiutare i titolari del trattamento nelle loro valutazioni d'impatto sulla protezione dei dati, il Garante per la protezione dei dati personali (GPDP) ha pubblicato sul suo sito delle linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7015994. Anche la *Commission Nationale de l'Informatique et des Libertés* (CNIL) mette a disposizione sul suo sito Internet il software libero PIA: https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil . È ora disponibile anche in lingua italiana: https://github.com/LINCnil/pia/tree/master/src/assets/i18n

dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. A titolo d'esempio, il regolamento cita tra l'altro la pseudonimizzazione, la cifratura e i mezzi in grado di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi. Il titolare del trattamento deve anche adottare misure per garantire che *«chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.»* (cfr. art. 32 § 4).

Da quest'obbligo di sicurezza deriva il **nuovo obbligo di notificare all'autorità di controllo le violazioni** dei dati personali. In alcuni casi questa violazione dovrà essere comunicata anche all'interessato:

- l'articolo 33 GDPR istituisce un sistema di notifica delle violazioni dei dati personali (*«data breaches»*). L'articolo 4 numero 12 GDPR definisce il concetto di violazione come *«la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati»*. Se una violazione può presentare un rischio per i diritti e le libertà delle persone fisiche, il responsabile del trattamento dovrà notificarla all'autorità di controllo, senza ingiustificato ritardo e, ove possibile, entro al massimo 72 ore (cfr. art. 33 § 1). Il responsabile del trattamento informa della violazione il titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. L'articolo 33 paragrafo 3 GDPR definisce il contenuto della notifica. Infine, il titolare del trattamento deve conservare la documentazione di ogni violazione in cui figurino le circostanze, le conseguenze e i provvedimenti adottati per porvi rimedio. Questa documentazione consente alle autorità di controllo di svolgere i loro incarichi e di esercitare i loro poteri;

- l'articolo 34 GDPR prevede invece le modalità e le condizioni che vanno rispettate nel comunicare agli interessati una violazione della sicurezza. Non prevede però alcun termine. L'idea di base è quella di permettere agli interessati di adottare, ove necessario, le misure che s'impongono per far cessare o attenuare gli effetti negativi che possono derivare dalla violazione dei dati.

L'articolo 37 GDPR definisce chi è obbligato a **designare un responsabile della protezione dei dati**[5]. In particolare: 1) le autorità pubbliche o un organismo pubblico, 2) le imprese che effettuano dei trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala 3) le imprese che effettuano trattamenti di dati sensibili. Inoltre, il regolamento consente alla legislazione dell'Unione o di uno Stato membro di esigere la designazione di un responsabile della protezione dei dati in casi non previsti dal GDPR. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati; questa possibilità esiste anche per le autorità pubbliche o gli organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione (art. 37 § 2 e 3). L'articolo 37 paragrafo 5 definisce le qualità professionali che il responsabile della protezione dei dati deve possedere.

Infine, il regolamento incoraggia l'elaborazione di codici di condotta (art. 40 e 41 GDPR) destinati a contribuire alla corretta applicazione del regolamento. Devono essere elaborati in funzione delle

[5] Cfr. Scheda informativa sulla figura del Responsabile della protezione dei dati personali http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4791784

specificità dei vari settori di trattamento e delle esigenze specifiche delle imprese. Tali codici saranno sottoposti all'autorità di protezione dei dati competente conformemente all'articolo 55 GDPR la quale si pronuncerà sulla loro conformità al regolamento. Gli articoli 42 e seguenti istituiscono un meccanismo di certificazione.

Obbligo di designare un rappresentante dei titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione (art. 27 GDPR)

Qualora si applichi l'articolo 3 paragrafo 2 GDPR, l'articolo 27 GDPR obbliga il titolare del trattamento e il responsabile del trattamento che non sono stabiliti nell'Unione a designare per scritto un rappresentante nell'Unione per le loro attività di trattamento soggette al regolamento. Il rappresentante deve essere stabilito in uno degli Stati membri in cui si trovano gli interessati e i cui dati personali sono trattati nell'ambito dell'offerta di beni o servizi o il cui comportamento è monitorato (art. 27 § 3).

Secondo il considerando 80 del GDPR, il rappresentante funge da interlocutore per le autorità di controllo (cfr. art. 58 GDPR) e per gli interessati su tutte le questioni relative al trattamento dei dati personali. Inoltre, dovrà tenere un registro di tutte le categorie di attività di trattamento dei dati personali svolte sotto la sua responsabilità (cfr. art. 30 GDPR). Potrebbe anche essere oggetto di misure attuative in caso di inadempienza al regolamento da parte del titolare del trattamento o del responsabile del trattamento. È tuttavia importante sottolineare che questo non incide affatto sulla responsabilità del titolare del trattamento o del responsabile del trattamento nei confronti delle autorità e degli interessati poiché questa designazione fa salve le azioni legali che potrebbero essere promosse contro lo stesso titolare del trattamento o responsabile del trattamento.

L'articolo 27 paragrafo 2 precisa che l'obbligo di designazione non si applica:

a) *«al trattamento se quest'ultimo è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10, ed è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento; oppure*
b) *alle autorità pubbliche o agli organismi pubblici.»*

Sanzioni previste

Contrariamente al diritto svizzero, il regolamento attribuisce alle autorità di controllo il potere d'infliggere **sanzioni amministrative pecuniarie** se sono riunite alcune condizioni. Ogni autorità di controllo dovrà provvedere affinché le sanzioni amministrative pecuniarie inflitte per le violazioni del GDPR siano **effettive, proporzionate e dissuasive**. Non va infatti dimenticato che il regolamento mette a disposizione tutta una serie di mezzi dissuasivi (cfr. art. 58 § 2 GDPR) come l'ingiunzione, l'intimazione, la limitazione provvisoria o definitiva del trattamento e gli ammonimenti. Tra questi, le autorità di protezione dei dati dovranno scegliere il mezzo più adatto a ottenere la conformità al regolamento.

È dunque solo come ultima ratio che i titolari di un trattamento rischiano sanzioni pecuniarie fino a 20 milioni di euro o corrispondenti al 4 per cento del loro fatturato mondiale totale annuo. L'articolo 83 GDPR elenca i fattori da considerare per fissare l'ammontare della sanzione.

Non bisogna tuttavia dimenticare che, se del caso, occorrerà anche risarcire gli eventuali danni subiti in seguito a un'azione legale.

A chi rivolgersi:

Dato che il regolamento è un atto giuridico europeo, vi consigliamo di rivolgere le vostre domande relative alla sua applicazione a un'autorità di protezione dei dati europea come il Garante per la protezione dei dati personali. Vi raccomandiamo inoltre di consultare il suo sito web che contiene linee guida, saggi e una guida all'applicazione del regolamento.