FISCALFOCUS.it
Direttore Antonio Gigliotti

Fiscal Approfondimento
N. 34 Del 29/05/2018

A cura della Redazione

Come cambia la gestione della privacy

Per professionisti e aziende

Categoria: **Privacy**
Sottocategoria: **Disposizioni generali**

Tavola sinottica

Sintesi

Il nuovo Regolamento Ue 679/2016 ha fatto il suo debutto ormai, dopo ben 2 anni dall'approvazione e con non poche difficoltà iniziali. Il Regolamento è stato, infatti, pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016 ed è entrato in vigore il 24 maggio 2016.
Le autorità avevano concesso un paio d'anni per la piena attuazione in tutti gli Stati membri.
Nonostante il periodo di adeguamento concesso, le nuove regole sulla privacy in Italia hanno debuttato il 25 maggio senza un quadro normativo di riferimento nazionale. **La data entro cui sarebbe scaduta la delega affidata al Governo per armonizzare le disposizioni nazionali sulla privacy in vigore e quelle europee, prevista al 21 maggio, è stata infatti prorogata al 21 agosto 2018.**
Di conseguenza per ora in riguardo alle regole da seguire per la protezione dei dati personali si dovrà far riferimento unicamente alle disposizioni dettate dal Regolamento europeo.

Il Focus

Nel presente contributo faremo un **focus sulle sanzioni** a cui si andrà incontro qualora non si siano attuate o completate in tempo utile le procedure di adeguamento alla normativa, **come cambia la dinamica dello studio o dell'azienda** con la nuova figura del Responsabile del trattamento dati all'interno dell'organigramma e dell'organizzazione aziendale e infine **come cambia la gestione dei dati personali all'interno dei processi.**
Analizzeremo inoltre i vari aspetti dello stato dell'arte della normativa.

Scadenze

- 25 maggio 2018 data piena attuazione Regolamento Ue 679/2016;
- 21 agosto 2018 scadenza delega Governo per armonizzare le disposizioni nazionali e europee.

Riferimenti Normativi

- Regolamento Ue 679/2016;
- D.Lgs. 196/2003 Codice della privacy.

Premessa

Partenza ad ostacoli per il nuovo Regolamento Ue 679/2016 sul trattamento dei dati che ha visto il via qualche giorno fa, venerdì 25 maggio, dopo ben due anni dall'approvazione.

Il Regolamento è stato pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016 ed è entrato in vigore il 24 maggio 2016, anche se le autorità hanno concesso poi un paio d'anni per la piena attuazione in tutti gli Stati membri.

Quadro normativo nazionale incerto

L'incipit in Italia è stato con non poche defiance, l'Italia è partita infatti, al contrario degli altri paesi europei senza un quadro nazionale di riferimento.

Nota bene

Non è arrivato in tempo utile quindi il quadro normativo a cui si doveva far affidamento per l'applicazione delle nuove regole in tutto il territorio nazionale, di conseguenza **si dovrà far riferimento unicamente alle disposizioni dettate dal Regolamento europeo.**

È stato, infatti, approvato solo in via preliminare il 21 marzo il Decreto che doveva andare a regolamentare le norme all'interno del territorio nazionale. L'iter legislativo andava completato entro il 21 maggio, data in cui sarebbe scaduta la delega al Governo per l'armonizzazione **delle disposizioni nazionali sulla privacy in vigore con quelle europee** proprio a ridosso della data della piena applicazione il nuovo Regolamento.

Eppure il quadro normativo attuale, su cui dovranno basarsi aziende e studi professionali nel nostro Paese non è ancora ben definito, l'intero iter si completerà, come preannunciato, **entro il 21 agosto 2018 ovvero la nuova data di scadenza della delega affidata al Governo.**

Le norme compatibili del vecchio Codice della privacy converranno con le disposizioni dettate dall'impianto europeo.

Difatti riportando un estratto della Legge n. 163 del 25 ottobre 2017 che delega il Governo al recepimento delle direttive europee e l'attuazione di altri atti dell'Unione Europea il Decreto avrebbe dovuto:

[…] 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.

Nota bene

C'è da comunque specificare che il Regolamento, essendo un atto dell'Ue direttamente vincolante per i cittadini **non aveva bisogno di alcun atto di recepimento a livello nazionale** per far la sua entrata ufficiale.

Ultimi step normativa nazionale

La discussione in merito al decreto è partita soltanto mercoledì 23 maggio e anche se la mancata approvazione ha portato con sé conseguenze e clima di incertezze si è preferito continuare verso un approfondimento, anche in riferimento alle molteplici questioni sollevate dal Garante della privacy come ad esempio:

Osservazioni Garante

- alcune incongruenze sulle disposizioni della normativa nazionale riguardo al limite di età dei minori di 16 anni;
- l'estensione di alcuni obblighi anche ad altre attività;
- il sistema sanzionatorio da definire, in particolar modo in riferimento alle disposizioni penali.

Vantaggi del nuovo Regolamento Ue sulla privacy

L'evoluzione della tecnologia e la globalizzazione portano con sé nuove sfide, la tecnologia attuale consente di utilizzare dati personali come mai in precedenza per lo svolgimento delle proprie attività.

I pilastri del nuovo cambiamento sono da un lato la protezione dei dati personali e dall'altro la libera circolazione dei medesimi all'interno dei confini dell'Unione Europea.

Il sistema vedrà le aziende e la PA caricate di nuove responsabilità considerato anche le notevoli sanzioni che come anzidetto potranno arrivare fino a 20 milioni di euro e al 4% del fatturato.

Principali innovazioni e nuove opportunità – Gli elementi principali in materia di protezione dei dati sono:
• **un'unica serie di norme in tutto il continente,** per garantire la certezza giuridica per le imprese e lo stesso livello di protezione dei dati in tutta l'UE per i cittadini;
• **applicazione delle stesse norme a tutte le imprese che offrono servizi nell'UE**, anche se aventi la propria sede al di fuori dell'UE;
• **diritti nuovi e più forti per i cittadini**: il diritto all'informazione, il diritto di accesso e il diritto all'oblio sono rafforzati. Il nuovo diritto alla portabilità dei dati consente ai cittadini di trasferire i propri dati da un'impresa all'altra. Ciò offrirà alle imprese nuove opportunità commerciali;
• **maggiore protezione contro le violazioni dei dati:** le imprese sono tenute a notificare entro 72 ore all'autorità di protezione dei dati le violazioni dei dati che mettono a rischio le persone;
• **norme rigorose e multe dissuasive:** tutte le autorità di protezione dei dati avranno il potere di infliggere **multe fino a un massimo di 20 milioni di euro** o, nel caso di un'impresa, **fino al 4%del fatturato annuo a livello mondiale.**

I vantaggi vanno quindi dall'avere un'unica autorità per la protezione dei dati, anche per attività svolte all'estero e norme che troveranno applicazione anche ai soggetti extra-europei che operano nell'Unione europea.

Con il nuovo Regolamento nuove opportunità di lavoro

L'applicazione del nuovo regolamento ha condotto a notevoli vantaggi anche in termini di nuovi posti di lavoro. L'applicazione delle nuove norme hanno generato la richiesta di **45mila esperti** tra data protection officer e **consulenti in materia di protezione dei dati.**

A chi si applica

TUTTI dovranno applicare le nuove norme, in tutto il territorio dell'Ue, dai grossi colossi quali Google alle banche, alle farmacie, le **PA, le Pmi e le organizzazioni no profit**, ovvero tutti coloro i quali, per lo svolgimento delle proprie mansioni, maneggiano dati degli utenti, anche quelli più basilari.

L'unica esclusione è prevista dai casi di seguito indicati:

ESCLUSIONE

Il Regolamento 679/2016 prevede, alla lettera c) del primo comma dell'articolo 2 "Ambito di applicazione materiale", l'esclusione dell'applicazione esclusivamente ai trattamenti di dati personali:

"(…) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;".

Step adeguamento

Ma sintetizziamo di seguito gli step da seguire per adeguarsi ed essere conformi:

1. **Individuazione dei ruoli e delle responsabilità** attraverso la designazione in tempi stretti del Responsabile della protezione dei dati (o **DPO – Data Protection Officer**) che in alcuni casi è obbligatoria e l'individuazione, sensibilizzazione e formazione di tutte le persone "attive" del processo - Individuare anche le singole responsabilità;
2. L'istituzione del **Registro delle attività del trattamento**, dove sono descritti i trattamenti effettuati e le procedure di sicurezza adottate;
3. **Analizzare e fissare gli adempimenti** previsti nel caso ad esempio di un data breach, ossia la notifica delle violazioni dei dati personali, (perdita, violazione ecc. di dati sensibili, protetti o riservati) o la valutazione d'impatto sulla protezione dei dati personali da effettuare i caso dal trattamento dei dati ne derivi un rischio elevato (consente di valutare gli aspetti relativi alla protezione dei dati, prima che questi vengano trattati);
4. **Definizione delle politiche di sicurezza** e valutazione dei rischi (determinazione del valore quantitativo o qualitativo dei rischi connessi ad una situazione concreta o minaccia conosciuta);
5. **Implementazione dei processi per l'esercizio dei diritti dell'interessato** (al fine di assicurarsi di aver adottato tutte le procedure idonee alla tutela dei diritti dell'interessato);
6. **Stesura/modifica della documentazione** (Tutta la documentazione deve essere necessariamente sempre aggiornata e completa);
7. **Adottare tutte le misure necessarie per la cyber security** (crittografia, pseudonimizzazione dati, backup dati, sicurezza password ecc.).

La nuova figura del DPO in azienda e negli studi professionali

- ⇨ Ho designato le figure chiave?
- ⇨ Ho formato il personale?
- ⇨ Devo nominare il DPO e con quali responsabilità?

Tel. 0968.425805 - E-mail: info@fiscal-focus.it - www.fiscal-focus.it -

Sono queste le domande che bisogna porsi all'interno di un'organizzazione aziendale o all'interno di studi professionali per la verifica della completa compliance alla normativa.

Attenzione

Per chi era obbligato per legge alla nomina e non l'ha effettuata è già in possibile sanzione, in quanto lo ricordiamo il Garante ha aperto pochi giorni prima dell'entrata ufficiale del Regolamento, la piattaforma di comunicazione dei dati del DPO.

Ero obbligato alla designazione?

Ebbene la comunicazione del DPO era obbligatoria se:

SONO TENUTI ALLA NOMINA DEL DPO (A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO):
• *istituti di credito*
• *imprese assicurative;*
• *sistemi di informazione creditizia;*
• *società finanziarie;*
• *società di informazioni commerciali;*
• ***società di revisione contabile**;*
• *società di recupero crediti;*
• *istituti di vigilanza che già hanno alcuni requisiti che devono rispettare sulla Data Protection (con le norme UNI 10891 - UNI CEI EN 50518 - Decreto del Ministero dell'Interno 04/06/2014 n. 115, Decreto del Ministero dell'Interno 01/01/2010 n. 269 e Disciplinare del Capo della Polizia);*
• *PMI che ha quale "core business" un'attività spinta di Marketing (email, call center, ecc...)*
• *partiti e movimenti politici; sindacati;*
• *società operanti nel settore delle "utilities"(telecomunicazioni, distribuzione di energia elettrica o gas);*
• *imprese di somministrazione di lavoro e ricerca del personale;*
• *società operanti nel settore della cura della salute (Case di cura, Cliniche...);*
• *società operanti nel settore della prevenzione/diagnostica sanitaria quali:* o *ospedali privati,* o *terme,* o ***laboratori di analisi mediche** (dove spesso l'applicazione della Data Protection non sempre è attuata, ad esempio per l'utilizzo di software obsoleti o di procedure di check in non conformi),*

o ***centri di riabilitazione***;
• *società di call center (che utilizzano dati di cittadini Europei anche se hanno sede fuori dall'Europa);*
• ***società che forniscono servizi informatici,*** *quali tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale;*
• *società che erogano servizi televisivi a pagamento*
• *caf e patronati;*
• ***Studi Associati*** *o* ***società di elaborazione paghe di professionisti associati.***
NON SONO TENUTI ALLA NOMINA DEL DPO (A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO):
• *Liberi professionisti* ***operanti in forma individuale*** *(****Avvocato****, Ingegnere, Architetto,* ***Commercialista*** *...);*
• *Agenti, rappresentanti e mediatori operanti non su larga scala;*
• *Imprese individuali o familiari;*
• *PMI, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con clienti, fornitori e dipendenti.*

Domanda

Ho nominato il Responsabile del trattamento dati quali mansioni dovrà ricoprire? E quali compiti dovrà svolgere all'interno della mia organizzazione?

SECONDO L'ARTICOLO 39

IL DPO DOVRÀ PRINCIPALMENTE:

INFORMARE E CONSIGLIARE il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

VERIFICARE l'attuazione e l'applicazione del Regolamento;

ATTRIBUIRE DELLE RESPONSABILITÀ, SENSIBILIZZARE E **FORMARE** il personale coinvolto nelle operazioni di trattamento;

GESTIRE GLI AUDIT INTERNI E FORNIRE PARERI in merito alla valutazione d'impatto sulla protezione dei dati;

SORVEGLIARE GLI ADEMPIMENTI relativi all'applicazione delle norme;

FUNGERE DA PUNTO DI CONTATTO PER GLI INTERESSATI in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;

FUNGERE DA PUNTO DI CONTATTO PER IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI OPPURE, EVENTUALMENTE, CONSULTARE L'AUTORITÀ DI PROPRIA INIZIATIVA.

I principi cardini del nuovo Regolamento

Fra i principi cardine del nuovo Regolamento, affinché il trattamento dei dati personali sia lecito e trasparente vi sono **l'obbligo di informare l'interessato** e la **raccolta del consenso**.

Leicità del trattamento	Art. 6	**Quando il trattamento è lecito?** Solo se l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità oppure: • il trattamento è **necessario** all'esecuzione di un **contratto** di cui l'interessato è parte o all'esecuzione di **misure precontrattuali** adottate su richiesta dello stesso; • il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il **titolare del trattamento**; • il trattamento è necessario per la salvaguardia degli **interessi vitali dell'interessato** o di un'altra persona fisica; • il trattamento è necessario per l'esecuzione di un **compito di interesse pubblico** o connesso all'**esercizio di pubblici poteri** di cui è investito il titolare del trattamento; • il trattamento è necessario per il perseguimento del **legittimo interesse del titolare** del trattamento o di terzi. A differenza del passato il bilanciamento fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato non spetta all'Autorità ma è compito dello stesso titolare. Trova così espressione il nuovo principio di "**responsabilizzazione**".
Forma del consenso	Art. 7	Il consenso non deve essere fornito per iscritto, sebbene la **forma scritta** sia l'unica a garantirne l'**inequivocabilità**. "*Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda **anche altre questioni**, la richiesta di consenso è presentata **in modo chiaramente distinguibile dalle altre materie**, in forma comprensibile e facilmente accessibile, utilizzando un **linguaggio semplice e chiaro***". L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato. Il consenso dovrebbe essere "*espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale". Va inoltre precisato che non basta il consenso non dovrà essere prestato in maniera sommaria ma come lo stesso considerando specifica: "Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste".*

Per quanto riguarda l'informativa invece il **titolare del trattamento** deve fornire all'interssato al trattamento, **nel momento in cui i dati personali sono ottenuti**, specifiche **informazioni** (c.d. **"obbligo di informativa"**).

Secondo l'art. 13 del Regolamento deve contenere le seguenti informazioni:

- l'identità e i dati di contatto del **titolare del trattamento** e, ove applicabile, del suo **rappresentante**;
- i dati di contatto del **responsabile della protezione dei dati**, ove applicabile;
- le **finalità del trattamento** cui sono destinati i dati personali nonché la **base giuridica del trattamento**. Si precisa che, ogni volta che le **finalità cambiano**, è necessario informarne l'interessato prima di procedere all'ulteriore trattamento;
- qualora il trattamento sia legittimato dal necessario perseguimento del **legittimo interesse del titolare** del trattamento o di terzi, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- gli eventuali **destinatari** o le eventuali **categorie di destinatari dei dati personali**;
- ove applicabile, l'**intenzione** del titolare del trattamento di **trasferire dati personali a un paese terzo** o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione.
- il **periodo di conservazione dei dati personali** oppure, se non è possibile, i **criteri utilizzati per determinare tale periodo**;
- l'**esistenza del diritto** dell'**interessato** di chiedere al titolare del trattamento l'**accesso ai dati** personali e la rettifica o la **cancellazione degli stessi** o la limitazione del trattamento che lo riguardano o di **opporsi al loro trattamento**, oltre al diritto alla portabilità dei dati;
- l'esistenza del **diritto di revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il **diritto di proporre reclamo** a un'autorità di controllo;
- se la comunicazione di dati personali è un **obbligo legale o contrattuale** oppure un requisito necessario per la **conclusione di un contratto**, e se l'interessato ha l'obbligo di fornire i dati personali nonché le **possibili conseguenze della mancata comunicazione di tali dati**;
- l'esistenza di un **processo decisionale automatizzato**, compresa la profilazione, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Nota bene

Art. 12 del Regolamento - Tutte le richiamate informazioni devono essere fornite in **forma scritta** e in **maniera coincisa**, trasparente, e con un **linguaggio semplice e chiaro**.

Maggiori tutele degli interessati

Bisogna inoltre effettuare un controllo sui diritti degli interessati che sono stati fortemente rafforzati dal nuovo Regolamento ampliandone anche, in alcuni casi, il perimetro di azione.

Sono in grado di garantirli?

Una importante riforma in riguardo alla tutela dei propri diritti in materia di privacy: ogni individuo potrà pretendere, infatti, che i propri dati personali siano trattati da terzi solo nel rispetto delle regole e dei principi stabiliti dalla legge e potrà esercitare inoltre i propri diritti in riguardo all'accesso, alla cancellazione e alla eventuale rettifica.

E' opportuno che i titolari di trattamento **adottino le misure tecniche e organizzative** eventualmente **necessarie per favorire l'esercizio dei diritti** e il riscontro alle richieste presentate dagli interessati.

Tali diritti sono posti al centro di ogni processo della nuova riforma, dal d**iritto all'accesso, alla cancellazione, alla rettifica, all'eventuale limitazione** dell'utilizzo stesso dei dati che lo riguardano fino al diritto alla **portabilità dei dati.**

ELENCO DIRITTI INTERESSATI

Diritto di accesso – Art.15	Diritto di accesso/ di copia da parte del titolare sui propri dati
Diritto di cancellazione (diritto all'oblio) - Art.17	Diritto alla cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo in casi specificamente individuati.
Diritto di limitazione del trattamento (art. 18)	Trattamento è illecito l'interessato contesta l'esattezza dei dati personali ecc.
Diritto alla portabilità dei dati (art. 20)	Trasferimento dei dati ad altro titolare
Diritto di opposizione - Articolo 21	Per alcune tipologie di trattamento di dati personali
Diritto di rettifica - Articolo 16	Diritto di ottenere dal titolare del trattamento la rettifica dei dati personali, e senza ingiustificato ritardo integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Sono tenuto ad effettuare la valutazione di impatto?

I titolari secondo il principio di "responsabilizzazione" **(o "*accountability*")** sono tenuti ad adottare **attività preventive (dimostrabili)**.

- Il titolare dovrà effettuare la **valutazione d'impatto sulla protezione dei dati** (detta anche **DPIA**, acronimo del nominativo inglese "Data Protection Impact Assessment");
- ogni qualvolta un tipo di trattamento preveda in particolare l'uso di nuove tecnologie, e che in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, può presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche.

In generale "*fatti salvi i casi in cui un trattamento rientra nel campo di applicazione di un'eccezione,* ***è necessario realizzare una valutazione d'impatto sulla protezione dei dati qualora un trattamento "possa presentare un rischio elevato""***.

QUANDO VA EFFETTUATA?

L'**articolo 35 del Regolamento** fornisce alcuni **esempi** di casi nei quali un trattamento ***"possa presentare rischi elevati"***:

- una valutazione sistematica e globale degli aspetti personali relativi a persone fisiche, basata sul **trattamento automatizzato**, compresa la **profilazione**;
- **un trattamento, su larga scala**, di categorie particolari di dati (**dati sensibili**), o di dati relativi a condanne penali e a reati;
- **operazioni di sorveglianza** sistematica di zone accessibile al pubblico su larga scala.

IL CONTENUTO MINIMO DELLA DPIA

IN PARTICOLARE UNA DPIA DEVE CONTENERE ALMENO:
• una **descrizione sistematica dei trattamenti previsti e delle finalità del trattamento**, compreso anche, eventualmente, l'interesse legittimo perseguito dal titolare del trattamento;
• una **valutazione della necessità e proporzionalità dei trattamenti** in relazione alle finalità;
• una **valutazione dei rischi per i diritti e le libertà** degli interessati;
• le **misure previste per affrontare i rischi**, comprese le garanzie, le misure di sicurezza e i meccanismi previsti al fine di garantire la protezione dei dati personali e dimostrare la conformità del trattamento al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Cyber security

Ho predisposto le adeguate misure di sicurezza?

Cosa dovranno fare, in sintesi, le aziende o i professionisti? Queste alcune domande in riguardo alla sicurezza informatica e non solo all'interno di aziende e uffici.

Secondo il nuovo regolamento europeo ogni azienda dovrà:

- effettuare un controllo interno;
- verificare il proprio livello di esposizione ai rischi;
- svolgere una serie di interventi per mitigare i rischi;
- innalzare il livello di tutela;
- documentare le scelte prese secondo un processo di accountability che caratterizza l'intero regolamento.

Attenzione

Fra gli adempimenti a cui dare priorità assoluta, nel processo di adeguamento al nuovo Regolamento Ue 679/2016, in uno studio professionale è sicuramente la messa in sicurezza dei dati personali da attacchi cibernetici e non solo, attraverso l'utilizzo di nuovi strumenti informatici o attraverso la definizione di misure organizzative interne.

SICUREZZA DEL TRATTAMENTO

Principio di sicurezza nell'art. 32 del GDPR

in base al quale il Titolare del trattamento e il Responsabile del trattamento

mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

MISURE DI SICUREZZA CHE COMPRENDONO

LA PSEUDONIMIZZAZIONE E LA CIFRATURA DEI DATI PERSONALI	**LA CAPACITÀ DI ASSICURARE SU BASE PERMANENTE** LA RISERVATEZZA, L'INTEGRITÀ, LA DISPONIBILITÀ E LA RESILIENZA DEI SISTEMI E DEI SERVIZI DI TRATTAMENTO	**LA CAPACITÀ DI RIPRISTINARE** TEMPESTIVAMENTE LA DISPONIBILITÀ E L'ACCESSO DEI DATI PERSONALI IN CASO DI INCIDENTE FISICO O TECNICO

UNA PROCEDURA PER TESTARE, VERIFICARE E VALUTARE

regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Come gestire una violazione o una perdita accidentale dei dati - Data Breach

Ma nel caso in cui non siano state adottate le misure minime necessarie sopra indicate (cyber security - che, lo ricordiamo, permetterebbero l'inutilizzabilità del dato nel caso in cui terze persone non autorizzate ne venissero in possesso, come ad esempio la cifratura dei dati ecc.) **quali sono gli adempimenti previsti per imprese e professionisti in caso di incidente informatico o di perdita dei dati? Come si deve comportare il personale addetto?**

1. Potrebbe accadere, infatti, in qualsiasi azienda o studio professionale che avvenga u**na perdita accidentale dei dati a seguito di un attacco informatico, un furto di una chiavetta USB, di un pc, ecc.**
   Ci sono dei virus (trojan ad esempio) il cui obbiettivo è rubare dati e informazioni dal pc con cui vengono in contatto e questo è il caso più diffuso e statisticamente più probabile che potrebbe accadere in un'azienda o in uno studio professionale come causa accidentale di perdita dei dati;
2. O potrebbe anche accadere ad esempio la **trafugazione di dati da personale addetto o non**;
3. **La distruzione accidentale a causa di un incendio, la cancellazione o una distruzione non voluta**, anche se in quest'ultimi casi si consiglia sempre di avere una copia digitale o addirittura di far uso di solo dati informatici magari anche cifrati, con backup periodici.

Partiamo dal presupposto che una perdita dei dati, seppur accidentale, non dovrebbe mai accadere, ma proprio perché come lo stesso Regolamento indica, il titolare del trattamento è

obbligato ad adottare tutte le misure necessarie ab origine affinché una tale situazione non possa mai verificarsi in azienda o in qualsiasi studio professionale, secondo il principio infatti del privacy by design ovvero del "prevenire anziché correggere".

Domanda

Ma se una tale previsione così nefasta, ovvero una perdita o distruzione accidentale dei dati, dovesse accadere, quali sono le procedure da intraprendere?

Nota bene

Fra i diversi obblighi del titolare vi è anche l'obbligo di comunicare eventuali violazioni di dati personali (**data breach**) all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati. Se il titolare ritiene, infatti, che il rischio per i diritti e le libertà degli interessati sia elevato, allora, secondo i casi indicati dall'**art. 34**, dovranno essere informati anche gli interessati del data breach, descrivendo con un linguaggio chiaro e semplice la natura della violazione.

OBBLIGO NOTIFICA – Art.33 → **al Garante della Privacy**

Entro 72 h e comunque "senza giustificato ritardo" da quando si è venuti a conoscenza della violazione ai propri sistemi informatici.

→ 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;
→ 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;
→ Descrivere le probabili conseguenze della violazione dei dati personali;
→ 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.

CONTENUTO NOTIFICA

NON È OBBLIGATORIA INVECE LA COMUNICAZIONE ALL'INTERESSATO SE È SODDISFATTA UNA DELLE SEGUENTI CONDIZIONI:
• Il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
• Il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
• La comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Quali sono le sanzioni per inadempienze, illeciti o per chi non si è adeguato?

Nonostante ancora non sia chiaro il quadro normativo di riferimento certo, la linea sarà dura, **le sanzioni**, che lo ricordiamo, sono state pesantemente inasprite, **troveranno piena applicazione già**

da subito, non lasciando alcuna via di fuga né per imprese, professionisti, PA, e neppure per le organizzazioni no profit ecc. neanche per errori di mera applicazione, di trascuranza o per la ben minima nefandezza.

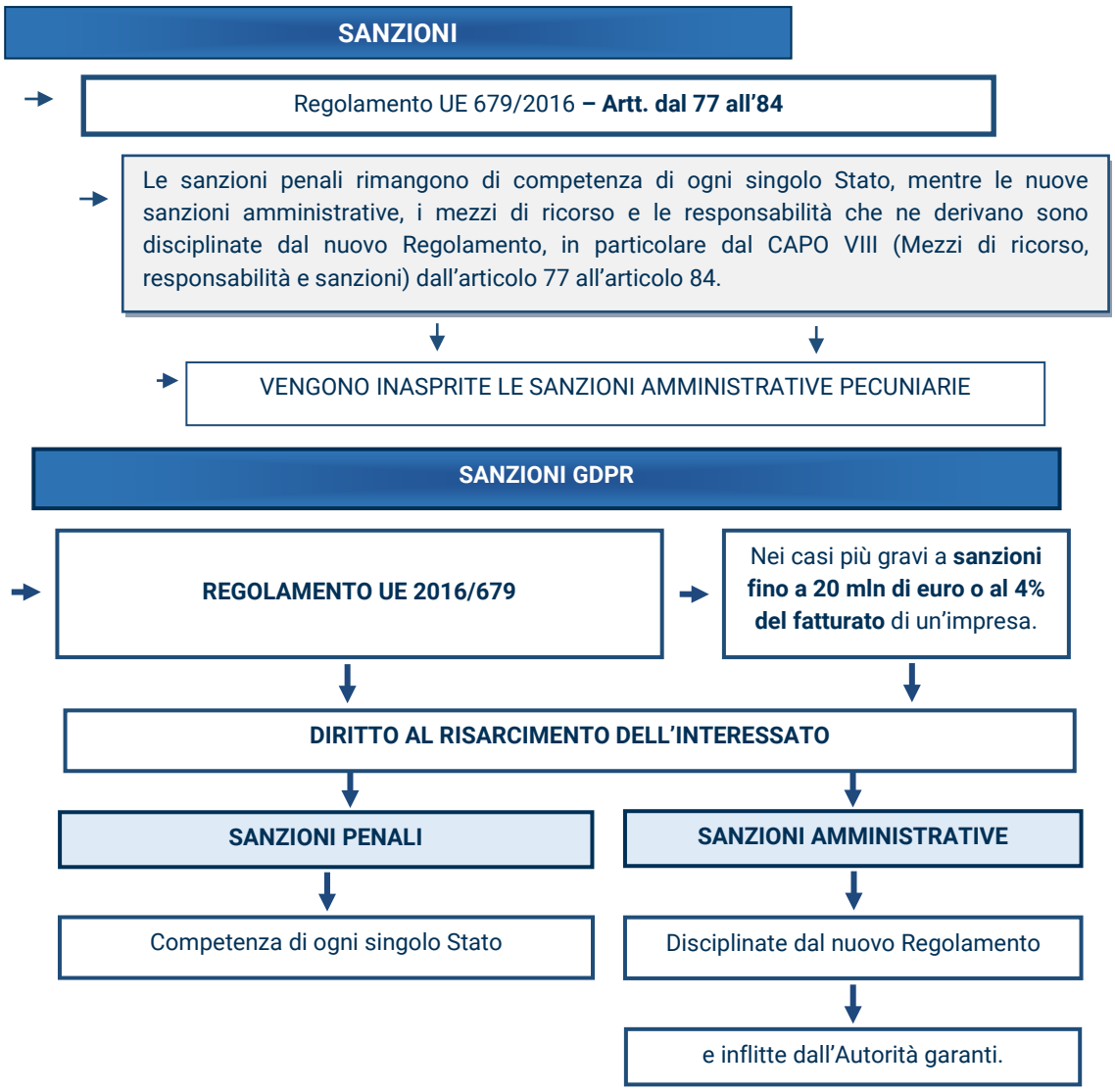
Nota bene

Il Garante, Antonello Soro, in una recente intervista rilasciata alla stampa specializzata (Italia oggi) ha rassicurato la platea dichiarando che l'applicazione del sistema sanzionatorio **sarà caratterizzato da un approccio gradualistico, congiuntamente o alternativamente alle misure inibitorie e prescrittive.**

Altro tasto dolente è rappresentato dalla **definizione degli illeciti penali**. In una prima versione, infatti, era decaduta interamente la parte riferita agli illeciti penali contenuta nel codice della privacy (D.Lgs. 196/2003).

Nota bene

Ora, invece, nello schema di Decreto che si trova al vaglio della Commissione Parlamentare ricompaiono le sanzioni già esistenti e si introducono **fattispecie del tutto nuove quali il reato di comunicazione e diffusione illecita a un rilevante numero di persone** e il **reato di acquisizione in maniera illecita di dati personali al fine di trarne profitto.**



OGNI AUTORITÀ DI VIGILANZA
(IN ITALIA IL GARANTE DELLA PRIVACY)

DEVE PROVVEDERE, IN OGNI SINGOLO CASO

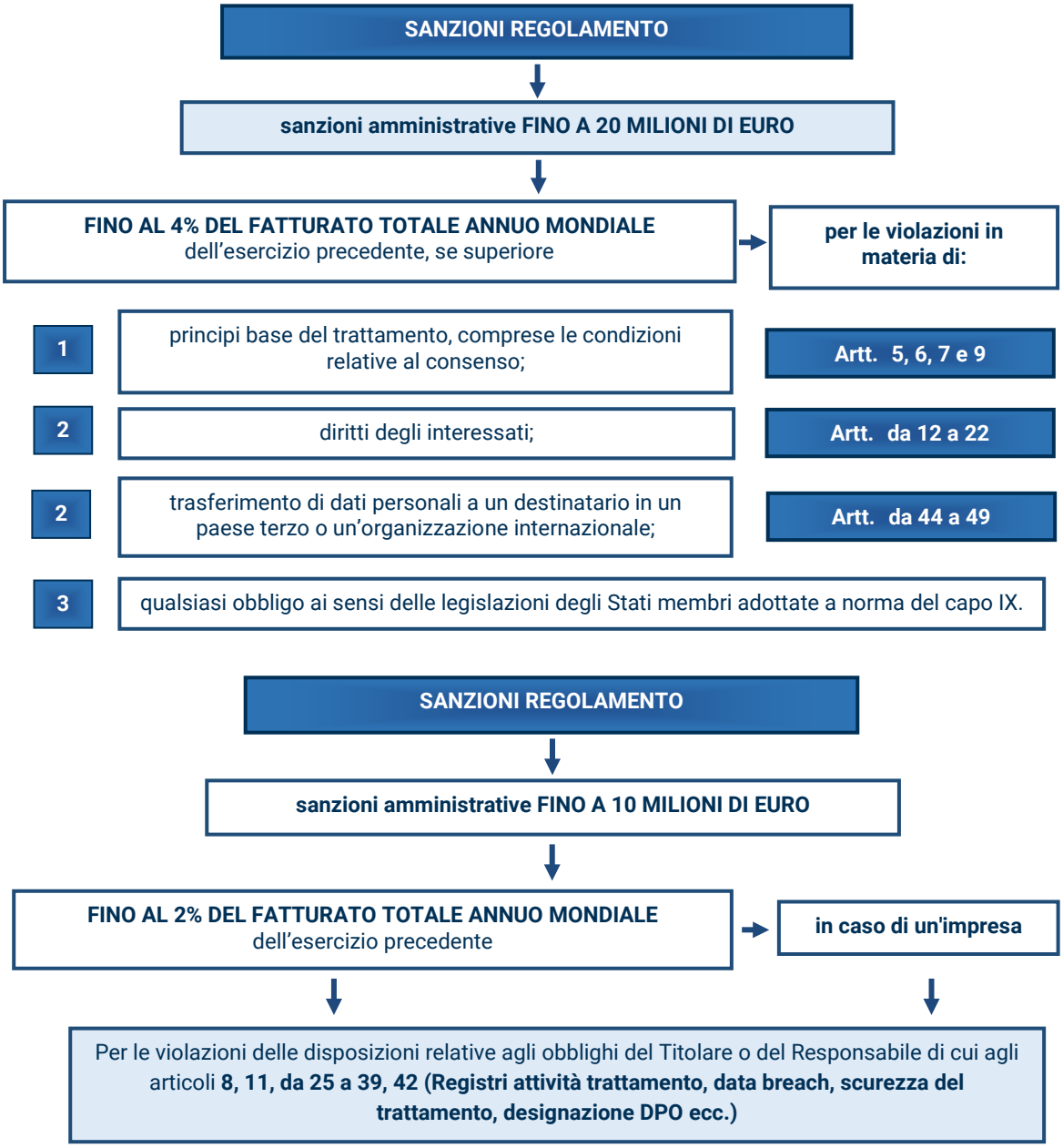
affinché **la sanzione amministrativa sia effettiva, proporzionata e dissuasiva**, secondo i parametri individuati nell'art. 83 Regolamento.

La valutazione dell'entità della sanzione amministrativa pecuniaria verrà fatta in base a:

- alla **natura, la gravità e la durata della violazione** tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
- il carattere **doloso o colposo** della violazione;
- alle **misure intraprese dal Titolare o dal Responsabile** per mitigare i danni subiti dagli interessati;
- il **grado di responsabilità** del Titolare o del Responsabile, anche sotto il profilo tecnico, e le misure organizzative attuate per prevenire le violazioni;
- **eventuali violazioni precedenti** commesse da parte del Titolare o del Responsabile;
- **al grado di cooperazione con l'autorità di vigilanza**, al fine di porre rimedio alla violazione e mitigarne i possibili effetti negativi;
- alle **categorie di dati personali** oggetto della violazione;
- ecc.

Attenzione

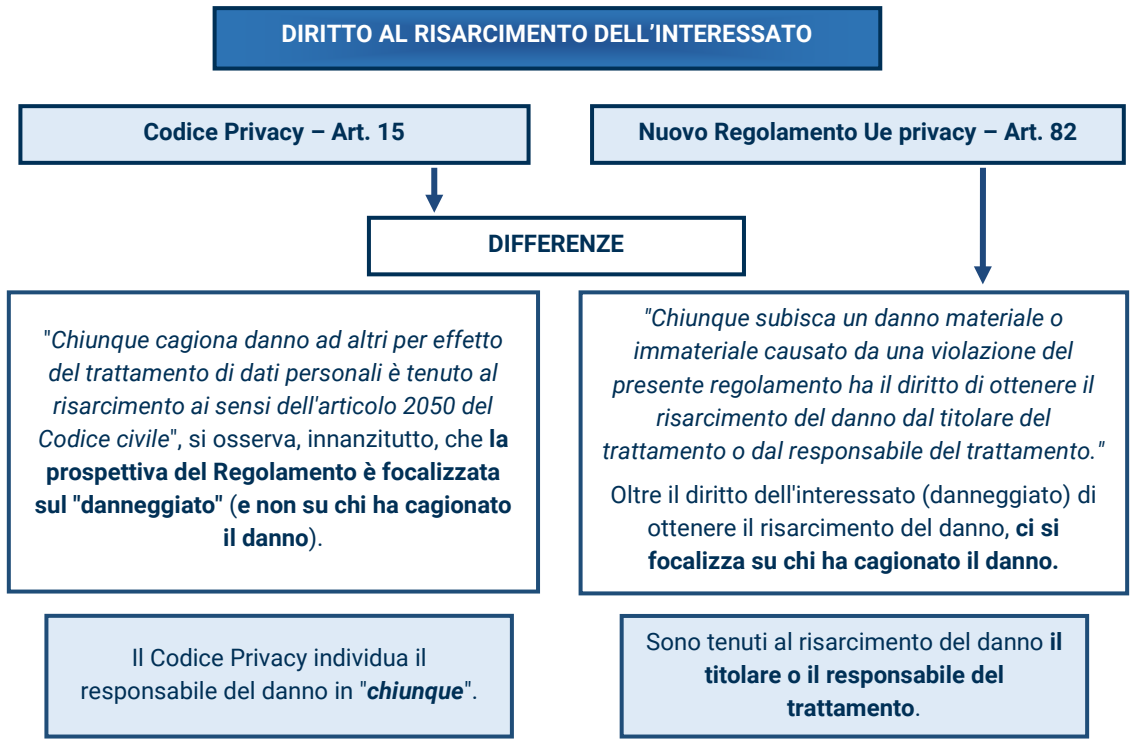
Due, inoltre, i "livelli" sanzionatori, uno in base il primo si applica per le violazioni delle disposizioni relative agli obblighi del Titolare o del Responsabile. Il secondo invece il più elevato, concerne le violazioni dei principi di base.



Attenzione

Se il Titolare o il Responsabile commetteranno più violazioni alle disposizioni del Regolamento connesse a una stessa operazione di trattamento di dati personali, l'importo totale della sanzione non dovrà superare l'importo indicato per la violazione più grave.

Il nuovo Regolamento Ue sulla privacy (all'art. 82) prevede inoltre che "chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento, ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento".



Osserva

Mentre il Codice Privacy individua il responsabile del danno in "*chiunque*"; il Regolamento indica il titolare e il responsabile del trattamento.

Tel. 0968.425805 - E-mail: info@fiscal-focus.it - www.fiscal-focus.it -