Opuscolo Privacy

Manuale ad uso del personale

Conforme ai sensi del Regolamento UE 679/2016 e al D.Lgs. 101/2018

INDICE

INQUADRAMENTO NORMATIVO IN MATERIA DI PRIVACY 3
PRIVACY E FONTI DEL DIRITTO EUROPEO 3
GENERAL DATA PROTECTION REGULATION 4
SCOPO E CAMPO DI APPLICAZIONE 5
SCOPO DEL GDPR 5
A CHI SI APPLICA? 5
ENTI DI CONTROLLO SULL'APPLICAZIONE DEL SISTEMA PRIVACY 5
DEFINIZIONI PROPEDEUTICHE 6
DATO PERSONALE 6
CATEGORIE DI DATI SECONDO LA NORMATIVA 6
ATTORI DEL TRATTAMENTO DEI DATI E RUOLI 7
L'INTERESSATO 7
IL TITOLARE DEL TRATTAMENTO 7
I CONTITOLARI 8
IL RESPONSABILE DEL TRATTAMENTO 8
IL SUB RESPONSABILE 9
SOGGETTI AUTORIZZATI AL TRATTAMENTO 9
DATA PROTECTION OFFICER (DPO) 10
TRATTAMENTO DEI DATI PERSONALI 11
TRATTAMENTO 11
I DIRITTI DEGLI INTERESSATI 12
OBBLIGHI DI COMUNICAZIONE 15
SISTEMA SANZIONATORIO 17
CONDIZIONI GENERALI PER INFLIGGERE SANZIONI AMMINISTRATIVE PECUNIARIE (art. 83) 17
SOGGETTI SANZIONABILI 17
SICUREZZA DEL TRATTAMENTO DEI DATI PERSONALI 18
TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI 19
DATA BREACH - VIOLAZIONE DEI DATI PERSONALI 21
PRIVACY BY DESIGN & PRIVACY BY DEFAULT 23
PRIVACY BY DESING (art.25 comma 1) 23
PRIVACY BY DEFAULT (art.25 comma 2) 23
DOCUMENTI DELLA PRIVACY 23
REGISTRO DEI TRATTAMENTI (art. 30 GDPR) 23
REGISTRO DELLE VIOLAZIONI 24
INFORMATIVA (artt.13 e14 GDPR) 24
VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) 25

INQUADRAMENTO NORMATIVO IN MATERIA DI PRIVACY

PRIVACY E FONTI DEL DIRITTO EUROPEO

La definizione di Privacy quale "diritto alla protezione dei dati di carattere personale" è stata sancita nel 1950 dalla CONVENZIONE EUROPEA (art.8) e ribadita nel 2000 dalla CARTA DEI DIRITTI FONDAMENTALI DELL'UNIONE EUROPEA**.**

DIRETTIVE: sono indirizzate agli Stati membri e sono obbligatorie in tutti i loro elementi, *vincolano* i destinatari (gli Stati) *solo riguardo al risultato da raggiungere,* lasciando alla loro discrezione la scelta dei mezzi e della forma.

Ciò significa che per sua natura, rappresenta un'indicazione della Commissione europea, che deve essere recepita con provvedimenti legislativi in ogni nazione.

REGOLAMENTI: hanno una portata generale, *sono obbligatori in tutti i loro elementi e direttamente applicabili*, cioè vincolano sia gli Stati che i singoli cittadini. Lo scopo dei regolamenti europei è quello di omogeneizzare le diverse normative dei singoli stati membri cioè di renderle più simili tra loro.

Nel 1995 la **Direttiva 95/46 CE "Tutela e libera circolazione dei dati personali"** ha dato origine, in Italia, alla **Legge 675 del 1996** al fine di garantire sia la circolazione dei dati che i diritti degli interessati *("le operazioni di trattamento dei dati sono al servizio dell'uomo e devono rispettare libertà e diritti fondamentali degli individui ed essere strumento di progresso economico e sociale")* e poi al **D.Lgs. 196 del 30 giugno 2003** "Codice in materia di protezione dei dati personali".

GENERAL DATA PROTECTION REGULATION

REGOLAMENTO EUROPEO IN MATERIA DEI DATI PERSONALI – REG. UE 679/2016

Nel 2016 è pubblicato, dopo quattro anni di lavori, il **Regolamento UE 2016/679 "GDPR"** acronimo di **General Data Protection Regulation**. Il Regolamento approvato dal Parlamento Europeo il 27 aprile 2016 è ed entrato in vigore il 25 maggio 2016, ed è diventato obbligatorio il **25 MAGGIO 2018**.

TRATTANDOSI DI UN REGOLAMENTO È DIRETTAMENTE APPLICABILE NEGLI STATI MEMBRI

In Italia l'adeguamento della normativa previgente al GDPR, è avvenuto modificando e abrogando parzialmente il DLgs.196/2003 "Codice privacy", prevedendo misure transitorie contenute all'interno del **D.Lgs 101 del 10.08.2018** (entrato in vigore il 19.09.2018),
dal titolo:

Decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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).

Ad oggi per avere un quadro completo, bisogna inoltre tener conto di:

- **Autorizzazioni e provvedimenti del Garante;**
- **Linee Guida del Gruppo di lavoro WP 29;**
- **Giurisprudenza.**

STRUTTURA DEL GDPR

È strutturato in **"CONSIDERANDO"** (spiegano alcuni articoli) e **ARTICOLI** veri e propri organizzati nei seguenti:

- **Capo I** Disposizioni generali
- **Capo II** Principi
- **Capo III** Diritti dell'interessato
- **Capo IV** Titolare del trattamento e responsabile del trattamento
- **Capo V** Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali
- **Capo VI** Autorità di controllo indipendenti
- **Capo VII** Cooperazione e coerenza

- **Capo VIII** Mezzi di ricorso, responsabilità e sanzioni
- **Capo IX** Disposizioni relative a specifiche situazioni di trattamento
- **Capo X** Atti delegati e atti di esecuzione
- **Capo XI** Disposizioni finali

SCOPO E CAMPO DI APPLICAZIONE

SCOPO DEL GDPR

Il Regolamento GDPR stabilisce **NORME** relative alla **PROTEZIONE DELLE PERSONE FISICHE** con riguardo al trattamento dei **DATI PERSONALI** (privacy, inteso come un diritto della persona), nonché norme relative alla libera circolazione dei dati personali, bilanciando la tutela dei due diritti (art.1); *sono esclusi i dati personali di **PERSONE GIURIDICHE** di diritto pubblico (es. Stato, Enti Pubblici) e di diritto privato (es. Spa, Associazioni, fondazioni, ecc)*.

A CHI SI APPLICA?

Il Regolamento GDPR si applica:

- **TITOLARI** e **RESPONSABILI** che siano stabiliti con le proprie attività IN UNO O PIÙ PAESI MEMBRI DELL'UNIONE EUROPEA, indipendentemente dal fatto che il trattamento sia effettuato o meno all'interno dell'Unione Europea.
- **TITOLARI E RESPONSABILI** stabiliti AL DI FUORI DELL'UNIONE EUROPEA ma con attività di trattamento dati relativi agli interessati che si trovano nel territorio europeo e che riguardano offerta di beni e servizi anche se non remunerati o attività di monitoraggio del comportamento.

ENTI DI CONTROLLO SULL'APPLICAZIONE DEL SISTEMA PRIVACY

Insieme all'**Autorità Garante Per La Protezione Dei Dati Personali**, l'attività di controllo viene effettuata anche dalla **Guardia di Finanza** e, nello specifico, dal **Nucleo Speciale Privacy.**

DEFINIZIONI PROPEDEUTICHE

DATO PERSONALE

art. 4 GDPR "QUALSIASI INFORMAZIONE RIGUARDANTE UNA PERSONA FISICA IDENTIFICATA O IDENTIFICABILE".

Si considera identificabile la persona fisica che può essere identificata direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

• *Considerando 27 GDPR*
Il presente regolamento non si applica ai dati personali delle persone decedute, tuttavia, gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute.

• *Considerando 30 GDPR*
Le persone fisiche possono essere associate a identificativi on-line prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli *indirizzi IP, i* marcatori temporanei come i *cookie*, gli identificativi di altro tipo come i *tag* di identificazione a radiofrequenza.
Tali identificativi possono lasciare tracce che in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare i profili delle persone fisiche e identificarle.

CATEGORIE DI DATI SECONDO LA NORMATIVA

- **Personali:** qualsiasi informazione riguardante una persona fisica identificata o identificabile direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, un dato relativo all'ubicazione, un identificativo online, uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- **Categorie particolari di dati personali**: origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

- ❖ **Genetici:** relativi alle caratteristiche genetiche ereditarie di una persona fisica forniscono informazioni univoche e sulla sua fisiologia o sulla sua salute e risultano in particolare dall'analisi di un suo campione biologico.
- ❖ **Biometrici:** ottenuti da un trattamento tecnico specifico e relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale.
- ❖ **Relativi alla salute:** attinenti alla salute fisica o mentale di una persona, compresa la prestazione di servizi di assistenza sanitaria che rivelano informazioni relative al suo stato di salute.

- **Relativi a condanne penali o reati:** relativi a condanne penali e ai reati o a connesse e misure di sicurezza **(artt. 9 e 10 GDPR).**

ATTORI DEL TRATTAMENTO DEI DATI E RUOLI

Il regolamento prevede diverse figure:

- INTERESSATO;
- TITOLARE DEL TRATTAMENTO;
- CONTITOLARE DEL TRATTAMENTO;
- RESPONSABILE DEL TRATTAMENTO;
- PERSONE AUTORIZZATE AL TRATTAMENTO;
- DATA PROTECTION OFFICER (DPO) o, nella traduzione italiana, "RESPONSABILE PROTEZIONE DATI" (RPD).

L'INTERESSATO

- **È IL PROPRIETARIO DEI DATI PERSONALI.**
- **AFFIDA AL TITOLARE DEL TRATTAMENTO I PROPRI DATI PERSONALI.**

IL TITOLARE DEL TRATTAMENTO

- è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che singolarmente o insieme ad altri, determina le **finalità** e i **mezzi** del trattamento dei dati personali (**art. 4** § **7 GDPR)**
- garantisce la protezione dei dati personali, infatti, l'ACCOUNTABILITY è esclusivamente del Titolare e dell'eventuale Contitolare.

ACCOUNTABILITY è la novità maggiore introdotta dal GDPR: il **PRINCIPIO DI RESPONSABILIZZAZIONE** attribuisce direttamente ai Titolari del trattamento il compito di assicurare ed essere in grado di comprovare il rispetto dei principi applicati al trattamento dei dati personali (art. 5 co.2, art. 7 co. 1, art. 15 GDPR).

Il **Titolare**:

- nelle persone giuridiche o autorità pubbliche, è individuato tenendo conto delle ordinarie attribuzioni degli organi previsti dall'atto costitutivo e dallo Statuto.
- può individuare soggetti di supporto, mediante delega di funzioni che deve essere puntuale e specifica (*per la pubblica amministrazione, riferimento art.97 della Costituzione*).

I CONTITOLARI

Quando due o più Titolari del trattamento determinano congiuntamente le **finalità** e i **mezzi** del trattamento essi sono definiti Contitolari **(art. 26 GDPR).**

I Contitolari determinano i loro ruoli con un **accordo interno,** che definisce in maniera inequivocabile le responsabilità di ognuno in merito all'osservanza degli obblighi nascenti dalla normativa privacy, con particolare riguardo:

- all'esercizio dei diritti dell'interessato;
- al rilascio dell'informativa agli interessati

L'accordo interno deve essere messo a disposizione degli interessati.

Gli interessati possono, comunque, rivolgersi Indifferentemente a uno qualsiasi dei titolari che operano congiuntamente. (art. 26 GDPR)

IL RESPONSABILE DEL TRATTAMENTO

E' la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. **(art. 4 § 8).**

Il Titolare deve accertare che il Responsabile presenti tutte le garanzie necessarie per essere in regola con la normativa privacy (in caso contrario si potrebbe configurare in capo al titolare una "culpa in eligendo"). **(art. 28 GDPR).**

QUESTA FIGURA È PRESENTE IN OGNI CASO DI OUTSOURCING, OSSIA OGNI QUALVOLTA ESTERNALIZZIAMO UN SERVIZIO (AD ES: COMMERCIALISTA, TECNICO INFORMATICO, CONSULENTE DEL LAVORO, ECC).

✓ **NOMINA DEL RESPONSABILE DEL TRATTAMENTO**

Il Titolare nomina il Responsabile del trattamento con un **contratto**, il quale deve prevedere:

- la materia e la durata del trattamento;
- la natura e le finalità del trattamento;

- il tipo di dati personali affidati in trattamento;
- le categorie degli interessati;
- obblighi e diritti del titolare del trattamento;
- eventuali Sub-responsabili.

✓ **CONTENUTI DEL CONTRATTO DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO**

Il **contratto** con cui il Titolare nomina il Responsabile del trattamento deve avere forma scritta e può essere predisposto anche in formato elettronico. Al suo interno deve prevedere:

- le istruzioni impartite dal Titolare per il trattamento dei dati personali;
- la garanzia da parte del Responsabile:
  - che le persone autorizzate al trattamento abbiano un adeguato impegno alla riservatezza;
  - di aver adottato idonee misure di sicurezza per il trattamento (cifratura, pseudonimizzazione, recupero da backup, ecc.);
  - di aver predisposto un'adeguata organizzazione per dare seguito alle eventuali richieste degli interessati nell'esercizio dei loro diritti;
  - della sua piena collaborazione con il Titolare, compreso consentire ad eventuali ispezioni di quest'ultimo **(art. 28 GDPR).**

✓ **LE RESPONSABILITÀ DEL RESPONSABILE DEL TRATTAMENTO**

Il Responsabile risponde per danno, se:

- non ha adempiuto agli obblighi previsti dal regolamento;
- ha agito senza rispettare le istruzioni del Titolare;
- ha disatteso le istruzioni ricevute dal Titolare;
- persegue proprie finalità con i dati di cui è responsabile (fatto considerato dal Garante molto grave rispetto a una semplice negligenza nel rapporto Titolare - Responsabile).

IL SUB RESPONSABILE

Il Responsabile del Trattamento può nominare a sua volta un Sub-responsabile per specifiche attività di trattamento nel rispetto degli stessi obblighi contrattuali che legano Il Titolare e il Responsabile primario. Tale nomina è consentita solo se vi è un'autorizzazione scritta da parte del Titolare.

ATTENZIONE!

Il Responsabile primario risponde dinnanzi al Titolare anche dell'inadempimento del Sub- responsabile ai fini del risarcimento di eventuali danni causati dal trattamento di quest'ultimo **(art. 28 GDPR).**

SOGGETTI AUTORIZZATI AL TRATTAMENTO

Sono quei soggetti che il Titolare adibisce al trattamento dei dati personali di cui ha l'accountability.

Tali soggetti **devono necessariamente essere istruiti** in maniera specifica **(art. 29, art. 32 co.4 GDPR)**

DATA PROTECTION OFFICER (DPO)

Il Titolare del trattamento o il Responsabile del trattamento **DEVONO** nominare un **DPO** nei seguenti casi:

- il trattamento è effettuato da una pubblica amministrazione;
- il trattamento richiede, per sua natura, ambito di applicazione o finalità, un monitoraggio regolare e sistematico degli interessati su larga scala;
- il trattamento è relativo a categorie particolari di dati su larga scala. **(art. 37 GDPR)**

REQUISITI DEL (DPO)

Il DPO può essere un soggetto esterno all'azienda o interno all'azienda.
Il DPO deve avere adeguate conoscenze specialistiche in materia di privacy, ma attualmente non esiste nessun albo di iscrizione.
Se il DPO è interno all'azienda, deve essere dotato di autonomia rispetto al Titolare del trattamento (**non vi deve essere conflitto di interessi**).
Un gruppo imprenditoriale può nominare un unico DPO se tutte le sedi del gruppo sono facilmente raggiungibili da questo.
I dati di contatto del DPO devono essere resi pubblici (nell'informativa) e la sua nomina deve essere comunicata al Garante per la Protezione dei dati Personali **(art. 37 GDPR).**

FUNZIONI DEL (DPO)

Il DPO:

- riferisce direttamente al vertice gerarchico del Titolare o del Responsabile;
- è tenuto al segreto e alla riservatezza **(art. 38 GDPR);**
- informa e fornisce consulenza al Titolare o al Responsabile del trattamento;
- controlla che le politiche aziendali in materia di privacy rispettino il Regolamento;
- fornisce un parere circa la valutazione di impatto sulla protezione dei dati (DPIA) (se viene richiesto);
- coopera con l'Autorità di Controllo;
- funge da punto di contatto per l'Autorità di Controllo;
- fa una valutazione del rischio privacy **(art. 39 GDPR).**

Il Titolare del trattamento o il Responsabile del trattamento, nel rapporto con il DPO, **DEVONO**:

- coinvolgerlo tempestivamente in tutte le questioni che riguardano la privacy;
- fornirgli le risorse necessarie per esercitare le sue funzioni;
- astenersi da impartire al DPO istruzioni per l'esecuzione dei suoi compiti;
- astenersi da rimuovere il DPO dal suo ruolo a causa dell'adempimento dei suoi compiti **(art. 38 GDPR).**

TRATTAMENTO DEI DATI PERSONALI

TRATTAMENTO

qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a **dati personali o insiemi di dati personali**, come:
Trattamento (di dati personali): **la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.**

PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

I **dati personali** devono essere:

- trattati in modo lecito, corretto e trasparente;
- trattati limitatamente al perseguimento della finalità per cui sono raccolti (limitazione della finalità);
- trattati nel minor numero possibile (minimizzazione dei dati);
- trattati mantenendone l'esattezza;
- trattati in maniera adeguatamente sicura ("pseudoniminizzazione") **(art. 5 GDPR)**

LIMITAZIONE DELLA FINALITA'

I dati raccolti per una finalità specifica possono essere ancora legittimamente trattati solo al fine:

- di perseguire un Pubblico interesse;
- ricerca scientifica;
- ricerca storica;
- ricerca statistica **(art. 5 GDPR).**

LICEITA' DEL TRATTAMENTO

Il **trattamento** è lecito, solo se è nella misura in cui, ricorre almeno una delle seguenti condizioni:

1. L'interessato ha espresso il **consenso** al trattamento dei propri dati personali per uno o più specifiche finalità;
2. è necessario all'**esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di **misure precontrattuali** adottate su richiesta dello stesso;
3. è necessario per adempiere un **obbligo legale** al quale è soggetto il Titolare del trattamento;
4. è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;
5. 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;

6. è necessario per il perseguimento del **legittimo interesse** del Titolare o di terzi a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore **(art. 6 GDPR).**

CONSENSO

E' qualsiasi manifestazione di volontà dell'interessato, effettuata mediante **dichiarazione scritta** o **azione positiva**, che deve essere (artt. 4 e 7 GDPR):

- libera
- specifica
- informata
- inequivocabile

Al momento del rilascio del consenso, l'interessato **DEVE** essere informato del diritto di revocare il proprio consenso in ogni momento. La revoca del consenso deve consistere in una procedura facile tanto quanto il rilascio del consenso stesso.
Non è legittimo subordinare l'esecuzione di un contratto al rilascio di un consenso per trattare dati che non sono necessari all'esecuzione del contratto stesso **(art. 7).**

CONSENSO DEI MINORI

In relazione all'offerta dei servizi della società dell'informazione (Web: faceboock, instagram, ecc), il trattamento dei dati del minore è lecito se il minore ha almeno 16 anni. Tuttavia gli Stati membri sono liberi di stabilire un'età inferiore **(art. 8 GDPR).**
In Italia, il D.Lgs. 196/2003 s.m.i. prevede che il trattamento dei dati dei minori sia lecito se il minore ha almeno 14 anni **(art. 2-quinquies D.Lgs 196/ 2003).**

I DIRITTI DEGLI INTERESSATI

Come già visto, alla base della accountability ci sono i principi per cui i dati personali devono essere trattati secondo liceità correttezza e trasparenza; raccolti per finalità determinate, esplicite e legittime; adeguati, pertinenti e limitati rispetto alle finalità;esatti; limitati nella conservazione; trattati garantendo sicurezza e integrità **(art. 5 GDPR).**
In particolare, i diritti degli interessati, prima sanciti all'art.13 del D.Lgs.196/2003**, abrogato in toto**, sono descritti nel GDPR dai seguenti:

- diritto di accesso **(art. 15 GDPR);**
- diritto di rettifica **(art. 16 GDPR);**
- diritto alla cancellazione o diritto all'oblio **(art. 17 GDPR);**
- diritto alla limitazione **(art. 18 GDPR);**
- diritto alla portabilità dei dati **(art. 20 GDPR);**
- diritto di opposizione **(art. 21 GDPR).**

IL DIRITTO DI ACCESSO (art.15)

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

1. finalità del trattamento;
2. categoria di dati personali trattati;
3. destinatari o le categorie di destinatari a cui i dati personali saranno comunicati (in particolare se destinatari di Paesi terzi o organizzazioni internazionali);
4. il periodo di conservazione dei dati personali previsto oppure se non è possibile, i criteri utilizzati per determinare tale periodo;
5. l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento:
   - la rettifica;
   - la cancellazione;
   - la limitazione del trattamento dei dati che lo riguardano o di opporsi al loro trattamento;
   - il diritto di proporre reclamo a un'Autorità di Controllo;
6. qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
7. l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22 GDPR (vedi approfondimento alla pagina successiva), e almeno in tali casi, informazioni significative sulla logica utilizzata, nonché sull'importanza e sulle conseguenze previste di tale trattamento per l'interessato;
8. in caso di trasferimento dei dati in un Paese terzo, l'esistenza di garanzie adeguate.

TUTTE LE SUDDETTE INFORMAZIONI (DA 1 A 8) NORMALMENTE SONO CONTENUTE NELL'INFORMATIVA.

- Su richiesta, il Titolare fornisce all'interessato una copia dei dati personali oggetto di trattamento.
- L'interessato può ottenere più di una copia dei propri dati, ma in questo caso deve pagare un contributo spese ragionevole.
- Le informazioni richieste possono essere fornite anche in formato elettronico.
- Il diritto di ottenere una copia dei dati non deve ledere i diritti e le libertà altrui.

PROFILAZIONE (art.22 GDPR)

E' una forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti:

- il rendimento professionale;
- la situazione economica;
- la salute;
- le preferenze personali;
- gli interessi;

- l'affidabilità;
- il comportamento;
- l'ubicazione;
- gli spostamenti **(art. 4 p.to 4)**

IL DIRITTO DI RETTIFICA (art.16)

- L'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo.
- L'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti.

IL DIRITTO ALLA CANCELLAZIONE O DIRITTO ALL'OBLIO (art.17)

L'interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza un ingiustificato ritardo, se sussiste almeno uno dei seguenti motivi:

1. i dati personali non sono più necessari per le finalità per cui erano stati raccolti;
2. vi è il ritiro del consenso ("opposizione a marketing diretto" - **art.21**);
3. i dati devono essere cancellati per un obbligo legale a cui è soggetto il Titolare del trattamento **(legge dello Stato)**;
4. il trattamento dei dati è illecito **(art. 6);**
5. il consenso è stato fornito quando l'interessato era minorenne per servizi della società dell'informazione **(art. 8).**

L'interessato **NON** ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano quando sussiste almeno uno dei seguenti motivi:

1. Il trattamento è necessario per l'esercizio della libertà di espressione e d'informazione;
2. Il trattamento è necessario per l'adempimento di un obbligo legale del Titolare;
3. Il trattamento è necessario per l'adempimento di un compito svolto nel pubblico interesse o nell'esercizio di pubblici poteri dal Titolare;
4. Il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica;
5. Il trattamento è necessario ai fini di archiviazione nel pubblico interesse di ricerca scientifica o storica o a fini statistici;
6. Il trattamento è necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

È previsto che il Titolare, ove un interessato eserciti il diritto all'oblio, adotti tutte le misure ragionevoli ad esempio deindicizzazione o anonimizzazione per soddisfare la richiesta, invitando altri Titolari coinvolti a cancellare qualsiasi link, copia o riproduzione di dati personali **(art. 17 GDPR).**

DIRITTO ALLA LIMITAZIONE (art.18)

L'interessato ha il diritto di ottenere dal Titolare del trattamento la limitazione del trattamento dei suoi dati personali quando:

- sono messi in stand by per consentire al Titolare di effettuare le opportune verifiche;

oppure

- in caso di trattamento illecito, si oppone alla cancellazione dei propri dati personali e chiede invece che ne sia limitato l'utilizzo;

oppure

- ha bisogno di quei dati per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, anche se il Titolare non avrebbe più bisogno di conservarli,

oppure

- ha esercitato il diritto di opposizione e si è in attesa di verificare la prevalenza tra diritti dell'interessato e i motivi di legittimo interesse del Titolare.

In tali situazioni, i dati sono «congelati» e conservati.

DIRITTO ALLA PORTABILITÀ DEI DATI PERSONALI (art.20)

L'interessato ha il diritto di ottenere la trasmissione diretta dei propri dati personali da un Titolare del trattamento ad un altro, se il trattamento si basa sul consenso dell'interessato o su un contratto ed è effettuato con mezzi automatizzati.
I dati devono essere trasferiti in un formato strutturato, di uso comune e leggibile da dispositivo automatico.

DIRITTO DI OPPOSIZIONE (art.21)

L'interessato può esercitare il diritto di opposizione in qualunque momento: l'opposizione fa cessare per sempre un determinato trattamento dei propri dati.

L'interessato ha il diritto di opporsi al trattamento dei suoi dati personali quando:

- il trattamento è effettuato in esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento *(l'interessato deve motivare l'opposizione);*
- il trattamento è effettuato per il perseguimento del legittimo interesse del Titolare o di terzi *(l'interessato deve motivare l'opposizione)*;
- il trattamento è effettuato per finalità di marketing diretto, includendo la profilazione, se presente, connessa alla stessa finalità (*l'interessato NON deve motivare l'opposizione*).

Il Titolare ha il diritto di continuare a trattare i dati personali nonostante l'opposizione se:

- dimostra di avere motivi legittimi che prevalgono sul diritto dell'interessato
- deve difendere un suo diritto in sede giudiziaria

OBBLIGHI DI COMUNICAZIONE

In caso di esercizio del diritto di rettifica, cancellazione o limitazione del trattamento da parte dell'interessato, **il Titolare informa con una COMUNICAZIONE ogni destinatario di quei dati personali.**
Se l'interessato lo richiede, il Titolare del trattamento gli comunica i soggetti che sono stati destinatari dei suoi dati personali **(art. 19 GDPR).**

Scheda di sintesi a mero scopo divulgativo. Per un quadro completo della materia, si rimanda alla legislazione in tema di protezione dei dati personali e ai provvedimenti dell'Autorità.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Conosci i principali diritti previsti dal Regolamento (UE) 2016/679?

Il Regolamento (articoli 15-22) riconosce importanti diritti in materia di protezione dei dati personali, che possono essere esercitati rivolgendosi al titolare del trattamento (soggetto pubblico, impresa, associazione, partito, persona fisica, ecc.).

Accesso ai propri dati personali

Hai il diritto di sapere se è in corso un trattamento di dati personali che ti riguardano e - se confermato - di ottenere una copia di tali dati ed essere informato su: l'origine dei dati; le categorie di dati personali trattate; i destinatari dei dati; le finalità del trattamento; l'esistenza di un processo decisionale automatizzato, compresa la profilazione; il periodo di conservazione dei dati; i diritti previsti dal Regolamento.

Rettifica, cancellazione, limitazione del trattamento, portabilità dei dati personali

Puoi chiedere - nei casi previsti dal Regolamento - che i dati personali a te riferiti siano rettificati o cancellati, o che ne venga limitato il trattamento. Puoi inoltre chiedere che i dati che tu hai fornito al titolare siano trasferiti ad un altro titolare («diritto alla portabilità»), nel caso in cui il trattamento si basi sul tuo consenso o su un contratto con te stipulato e venga effettuato con mezzi automatizzati .

Opposizione al trattamento

Puoi opporti al trattamento dei tuoi dati personali per motivi connessi alla tua situazione particolare, da specificare nella richiesta; oppure senza necessità di motivare l'opposizione, quando i tuoi dati sono trattati per finalità di marketing diretto.

Come si esercitano questi diritti?

Puoi presentare, gratuitamente e senza particolari formalità (per esempio, tramite posta elettronica, posta raccomandata, ecc.), una richiesta di esercizio dei diritti al titolare del trattamento (sul sito www.garanteprivacy.it è disponibile un modulo facsimile) . Il titolare del trattamento è tenuto entro 1 mese a rispondere alla richiesta, o a comunicare un eventuale ritardo nella risposta in caso di richieste numerose e/o complesse (la proroga non può comunque superare i 2 mesi). Se la risposta non perviene nei tempi indicati o non la ritieni soddisfacente, puoi rivolgerti al Garante per la protezione dei dati personali, mediante un reclamo ai sensi dell'art. 77 del Regolamento, oppure all'autorità giudiziaria.

FONTE: WWW.GARANTEPRIVACY.IT

SISTEMA SANZIONATORIO

CONDIZIONI GENERALI PER INFLIGGERE SANZIONI AMMINISTRATIVE PECUNIARIE (art. 83)

L'Autorità di Controllo infligge sanzioni amministrative pecuniarie che devono essere: **effettive, proporzionate, dissuasive.**

Quando l'Autorità di Controllo infligge una sanzione, tiene conto:

- della natura, della gravità e della durata della violazione (numero degli interessati lesi);
- del dolo o della colpa;
- delle misure riparatorie poste in essere successivamente;
- del grado di responsabilità (tenendo conto delle misure tecniche di sicurezza adottate);
- della eventuale reiterazione della violazione;
- del grado di cooperazione con l'Autorità di Controllo;
- della categoria di dati personali violati;
- se è stata notificata la violazione al Garante;
- se sono stati rispettati precedenti provvedimenti individuali del Garante;
- se si aderisce a codici di condotta o a meccanismi di certificazione;
- delle circostanze attenuanti o aggravanti (benefici finanziari o perdite evitate).

L'Autorità Garante, oltre ad infliggere sanzioni, ha il potere **(art.58)** di:

- rivolgere a Titolari e Responsabili avvertimenti, ammonimenti e ingiunzioni (attraverso delle prescrizioni);
- limitare in modo temporaneo o permanente il trattamento dei dati personali;
- ordinare l'interruzione di un trasferimento dati verso un'organizzazione internazionale o un paese terzo;
- revocare certificazioni.

SOGGETTI SANZIONABILI

Le sanzioni si applicano:
· al Titolare e al Responsabile del trattamento (sia persone fisiche sia persone giuridiche). Nelle società la persona fisica, infatti, è delegata dalla persona giuridica ad agire per suo conto e a suo nome in merito al trattamento dei dati personali;
· agli organismi accreditati deputati al controllo o al monitoraggio dei Codici di condotta e al rilascio delle
Certificazioni **(articolo 41).**

Ovviamente, IN CASO DI ILLECITO PENALE LA RESPONSABILITÀ È PERSONALE.

SANZIONI AMMINISTRATIVE PECUNIARIE

Fino a 10.000.000 € o, per le imprese, fino **al 2% del fatturato mondiale totale annuo** dell'esercizio
precedente, per violazioni relative a:

- obblighi del Titolare e del Responsabile del trattamento (artt. 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33,34, 35, 36, 37, 38, 39, 42 e 43);
- obblighi dell'organismo di certificazione (artt. 42 e 43);
- obblighi dell'organismo di controllo (art. 41 comma 4).

Fino a 20.000.000 € o, per le imprese, fino **al 4% del fatturato mondiale totale annuo** dell'esercizio
precedente, per violazioni relative a:

- i principi di base del trattamento, comprese le condizioni relative al consenso (artt. 5, 6, 7 e 9);
- i diritti degli interessati (artt. da 12 a 22);
- i trasferimenti di dati personali a un destinatario in un Paese terzo o un'organizzazione internazionale (artt. da 44 a 49);
- gli obblighi ai sensi delle legislazioni degli Stati membri (artt. da 85 a 91);
- inosservanza di ordini o limitazioni da parte dell'Autorità di Controllo (art. 58).

SICUREZZA DEL TRATTAMENTO DEI DATI PERSONALI

Il Titolare e il Responsabile del trattamento devono porre in essere misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio che comprendono:

- la pseudonimizzazione (vedi approfondimento alla tabella successiva) e la cifratura.
- la capacità di assicurare sempre 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 ai 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.

L'adesione a un codice di condotta approvato (art.40) o a un meccanismo di certificazione approvato (art.42), può essere utilizzata come elemento per dimostrare la conformità ai requisiti di sicurezza **(art.32 GDPR).**

PSEUDONIMIZZAZIONE (art. 4 punto 5 GDPR)

E' il trattamento dei dati personali in modo tale che questi non possano più essere attribuiti a un interessato

specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI

Il trasferimento di dati personali verso un Paese terzo (o un'organizzazione internazionale) è ammesso se la Commissione Europea ha deciso che il Paese terzo garantisce un livello di protezione adeguato dei dati personali.

In questo caso il trasferimento non necessita di Autorizzazioni specifiche da parte del Garante.

Nel sito del Garante vi è l'elenco dei Paesi terzi per i quali è stata adottata una **DECISIONE DI ADEGUATEZZA (art.45 GDPR)**:

- Andorra;
- Argentina;
- Australia;
- Canada;
- Faer Oer;
- Guernsey;
- Isola di Man;
- Israele;
- Jersey;
- Nuova Zelanda;
- Svizzera;
- Uruguay;
- USA.

In mancanza di una decisione di adeguatezza, il Titolare o il Responsabile del trattamento può trasferire i dati in un Paese terzo solo se:

- ✓ fornisce Garanzie adeguate
- ✓ gli interessati dispongono di diritti azionabili e mezzi di ricorso effettivi

Nello specifico, in mancanza di una decisione di adeguatezza i dati possono essere trasferiti se si verifica una delle seguenti condizioni **(art. 46 GDPR)**:

a. l'adesione a un **codice di condotta approvato**, unitamente all'impegno vincolante ed esecutivo di Titolare o Responsabile nel Paese terzo ad applicare le garanzie adeguate anche per quanto riguarda i diritti degli interessati.
b. il possesso di una **certificazione** riferita a un meccanismo approvato, unitamente all'impegno vincolante ed esecutivo di Titolare o Responsabile nel Paese terzo ad applicare le garanzie adeguate anche per quanto riguarda i diritti degli interessati.

c. l'adozione di **clausole contrattuali tipo** predisposte dalla Commissione Europea e disponibili sul sito del Garante
   - possono essere inserite nel contratto con il Responsabile
   - garantiscono che i dati saranno trattati conformemente al Regolamento anche nel Paese terzo.

d. il rispetto di **norme vincolanti d'impresa** (ossia documenti che stabiliscono principi vincolanti al cui

e. rispetto sono tenute tutte le società appartenenti a uno stesso gruppo d'imprese) che
   - incorporano i principi fondamentali in materia di protezione dei dati personali;
   - sono autorizzate dall'Autorità Garante a seguito di una procedura che prevede la collaborazione tra le
   Autorità Garanti degli Stati membri coinvolti.

In ogni caso, il trasferimento di dati personali verso un Paese terzo, in assenza di adeguate garanzie, è **ammesso** solo in situazioni particolari **(art. 49)**:

- quando vi è il consenso esplicito dell'l'interessato, che deve essere informato della mancanza di garanzie adeguate e dei possibili rischi.
- quando il trasferimento è necessario per l'esecuzione di misure precontrattuali o per concludere un contratto stipulato tra il Titolare e l'interessato.
- quando il trasferimento è necessario per l'esecuzione di misure precontrattuali o per concludere un contratto stipulato tra il Titolare e un terzo a favore dell'interessato.
- quando il trasferimento è necessario per importanti motivi d'interesse pubblico (es. cooperazioni internazionali).
- quando il trasferimento è necessario per esercitare un diritto in sede giudiziaria.
- quando il trasferimento è necessario per tutelare gli interessi vitali dell'interessato o di altre persone e l'interessato si trova nell'incapacità fisica o giuridica di prestare il proprio consenso.
- quando il trasferimento è effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può essere consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse.
- quando il trasferimento non è ripetitivo, riguarda un numero limitato di interessati ed è necessario per il perseguimento degli interessi legittimi del Titolare (il Titolare deve fornire adeguate garanzie e i diritti dell'interessato non devono prevalere).

DATA BREACH - VIOLAZIONE DEI DATI PERSONALI

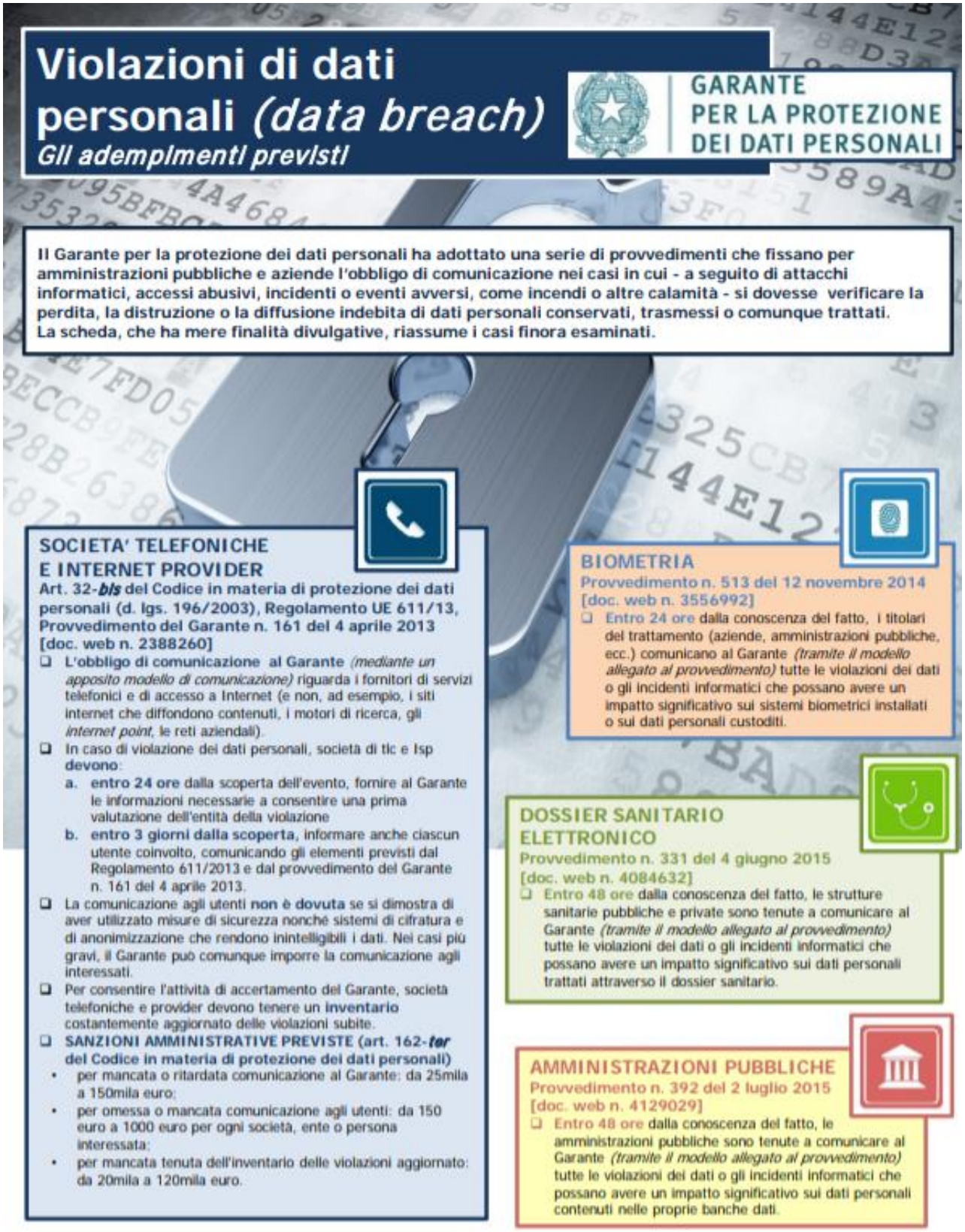
In caso di **violazione** dei dati personali (**Data Breach**) il Titolare del Trattamento deve:

1. **NOTIFICARE** la violazione al Garante entro 72 ore dal momento in cui ne è venuto a conoscenza **(art. 33)**.

Nella comunicazione devono essere indicati:
· la natura della violazione;
· la categoria dei dati violati;
· il numero degli interessati coinvolti;
· i dati di contatto del DPO (se nominato);
· le probabili conseguenze della violazione;
· le misure immediatamente adottate per porre rimedio.
Qualora la notifica non sia effettuata entro 72 ore, devono essere indicati i motivi del ritardo.
Il Responsabile del trattamento, dopo essere venuto a conoscenza di una violazione, deve informare il Titolare senza ingiustificato ritardo.

IL TITOLARE DEL TRATTAMENTO DEVE, COMUNQUE, DOCUMENTARE QUALSIASI VIOLAZIONE DEI DATI PERSONALI.

2. **COMUNICARE** la violazione all'interessato senza ingiustificato ritardo **(art.34)**.
Tale comunicazione può essere omessa se:
· Il Titolare ha posto in essere misure tecniche e organizzative adatte a proteggere i dati personali oggetto della violazione (es. cifratura);
· Il Titolare ha, dopo la violazione, adottato misure atte a scongiurare la violazione dei diritti e delle libertà degli interessati coinvolti;
· La comunicazione richiederebbe sforzi spropositati (numero elevato degli interessati coinvolti), in questo caso si procede con una comunicazione pubblica.



FONTE: WWW.GARANTEPRIVACY.IT

PRIVACY BY DESIGN & PRIVACY BY DEFAULT

Tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto, delle finalità del trattamento, dei diversi possibili rischi per i diritti e le libertà degli interessati,
il **Titolare del trattamento**, deve organizzare la sua attività mettendo in atto misure tecniche idonee ad attuare in modo efficace i principi di protezione dei dati e la tutela dei diritti degli interessati, quali:
· la **pseudonimizzazione** dei dati
· la **minimizzazione** dei dati.

PRIVACY BY DESING (art.25 comma 1)

Tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto, delle finalità del trattamento, dei diversi possibili rischi per i diritti e le libertà degli interessati.
Il **Titolare del trattamento** deve garantire che, per **impostazione predefinita**, verranno trattati solo i dati personali necessari per ogni specifica finalità (minimizzazione), tale obbligo vale per:
· la quantità dei dati personali;
· la portata del trattamento dei dati personali;
· il periodo di conservazione dei dati personali;
· l'accessibilità ai dati personali.

PRIVACY BY DEFAULT (art.25 comma 2)

Per cercare di conformarsi a questi principi ci si può rivolgere a procedure di Certificazione che, però, non fanno venir meno la responsabilità del Titolare del trattamento.

DOCUMENTI DELLA PRIVACY

REGISTRO DEI TRATTAMENTI (art. 30 GDPR)

Deve essere **obbligatoriamente** tenuto da:
- Imprese con più di 250 dipendenti;
- Imprese con meno di 250 dipendenti che effettuano un trattamento che possa comportare un rischio per i diritti e le libertà degli interessati;
- Imprese con meno di 250 dipendenti che effettuano un trattamento di dati personali non occasionale;
- Imprese con meno di 250 dipendenti che effettuano un trattamento di dati personali particolari.

Deve essere tenuto da:

- Titolare,
- Contitolare
- Responsabile del trattamento (deve tenere tanti registri quanti sono i Titolari per cui opera).

Deve essere tenuto in forma scritta, anche in formato elettronico.
Deve essere messo a disposizione dell'Autorità Garante qualora ne faccia richiesta.

Contenuti Del Registro Dei Trattamenti
Il Registro dei Trattamenti deve contenere:

- Il nome del Titolare, del Contitolare, del Rappresentante, del Responsabile e del DPO;
- Le finalità del trattamento;
- Le categorie degli interessati;
- Le categorie dei dati personali;
- Le categorie dei destinatari;
- I Paesi terzi in cui vengono trasferiti i dati;
- I termini per la cancellazione dei dati;
- La descrizione delle misure di sicurezza.

REGISTRO DELLE VIOLAZIONI

Il Registro delle violazioni:

- deve essere tenuto dal **Titolare.**
- deve essere tenuto in forma scritta, anche in formato elettronico.
- deve essere messo a disposizione dell'Autorità Garante qualora ne faccia richiesta.

Contenuti del Registro delle violazioni:
Il registro delle violazioni deve contenere:

- la descrizione della violazione avvenuta;
- le possibili conseguenze della violazione;
- i provvedimenti adottati per porre rimedio.

Il GDPR non disciplina in maniera dettagliata la tenuta di questo registro ma la necessità di questo si evince dall'**articolo 33 comma 5.**

INFORMATIVA (artt.13 e14 GDPR)

Deve essere fornita **obbligatoriamente** dal Titolare nel momento in cui i dati personali sono raccolti.
L'informativa cambia se:

- i dati personali siano stati raccolti presso l'interessato **(articolo 13)**
- i dati personali non siano stati raccolti presso l'interessato **(articolo 14)**

In questo caso nell'informativa:

- deve essere indicata la fonte dei dati personali.

- deve essere fornita all'interessato in tempi ragionevoli e comunque non oltre un mese dalla raccolta dei dati.

Contenuti dell'informativa (art. 13 GDPR)
L'informativa deve contenere:

1. Il nome e i dati di contatto del Titolare del Trattamento, del suo eventuale Rappresentante del DPO se nominato;
2. Le finalità del trattamento;
3. la base giuridica del trattamento, se si tratta del perseguimento di legittimi interessi esplicitare quali;
4. Le categorie di destinatari dei dati personali;
5. Se i dati vengono trasferiti i verso un Paese terzo precisando quale e le garanzie adottate;
6. Il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinarlo;
7. L'esistenza dei diritti fondamentali di ogni interessato e la possibilità di esercitarli;
8. Il diritto di revocare il consenso in qualsiasi momento;
9. Il diritto di presentare reclamo all'Autorità di Controllo;
10. L'esistenza di obblighi legali o contrattuali o di requisiti necessari per la conclusione di un contratto che determinano la necessità per l'interessato di comunicare i propri dati personali, nonché le possibili conseguenze dalla mancata comunicazione;
11. L'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, le informazioni sulla logica utilizzata e le conseguenze previste di tale trattamento per l'interessato.

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

Il Titolare, prima di effettuare il trattamento, deve effettuare una **DPIA** quando il trattamento prevede l'uso di nuove tecnologie e comporta un rischio elevato per i diritti e le libertà delle persone fisiche.
E'**obbligatoria** nei seguenti casi:

- quando viene fatta **profilazione** sulla quale si fondano decisioni che hanno effetti giuridici significativi sugli Interessati;
- quando viene effettuato un trattamento su **larga scala** di **dati particolari;**
- quando viene effettua **sorveglianza sistematica** e su **larga scala** di una zona accessibile al pubblico.

Contenuti della DPIA (ar.35 GDPR)
Deve contenere:

- una descrizione sistematica dei trattamenti effettuati;
- una descrizione sistematica delle finalità di trattamento;
- una valutazione delle 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 derivanti dal trattamento e per garantire la protezione dei dati personali.

Il Titolare quando svolge una DPIA consulta il DPO. La DPIA deve essere aggiornata in caso di modifica variazione dei trattamenti.