La responsabilità penale ed amministrativa nel Regolamento UE 2016/679 e nel Codice della Privacy

23 marzo 2021

Alberto Bulzatti

Alberto Bulzatti, docente e ingegnere, DPO, consulente tecnico per il Tribunale di Venezia, esperto di informatica forense, di privacy e di tecnologie applicate alla comunicazione.

- Cert. Istruttore Cisco Systems
- Master di Ingegneria Forense
- Master Privacy Officer e Consulente della Privacy

Ordine degli Ingegneri di Venezia
Data Protection Officer
Responsabile della transizione digitale
Membro Commissione Ingegneria Forense
Membro Commissione Informazione e Comunicazione


Yes
No

QUALI SONO LE CONSEGUENZE PER UN TRATTAMENTO DI DATI PERSONALI CHE HA CAGIONATO UN DANNO FISICO, MATERIALE O IMMATERIALE AD UN INTERESSATO?

Qualche definizione

Si fa riferimento alle norme relative alla protezione delle **persone fisiche** con riguardo al **trattamento** dei **dati personali**, nonché a norme relative alla **libera circolazione** di tali dati.

GDPR

Dato personale

[*Art.4 Definizioni –GDPR*]

Qualsiasi informazione riguardante una persona fisica **identificata** o **identificabile** […] 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.

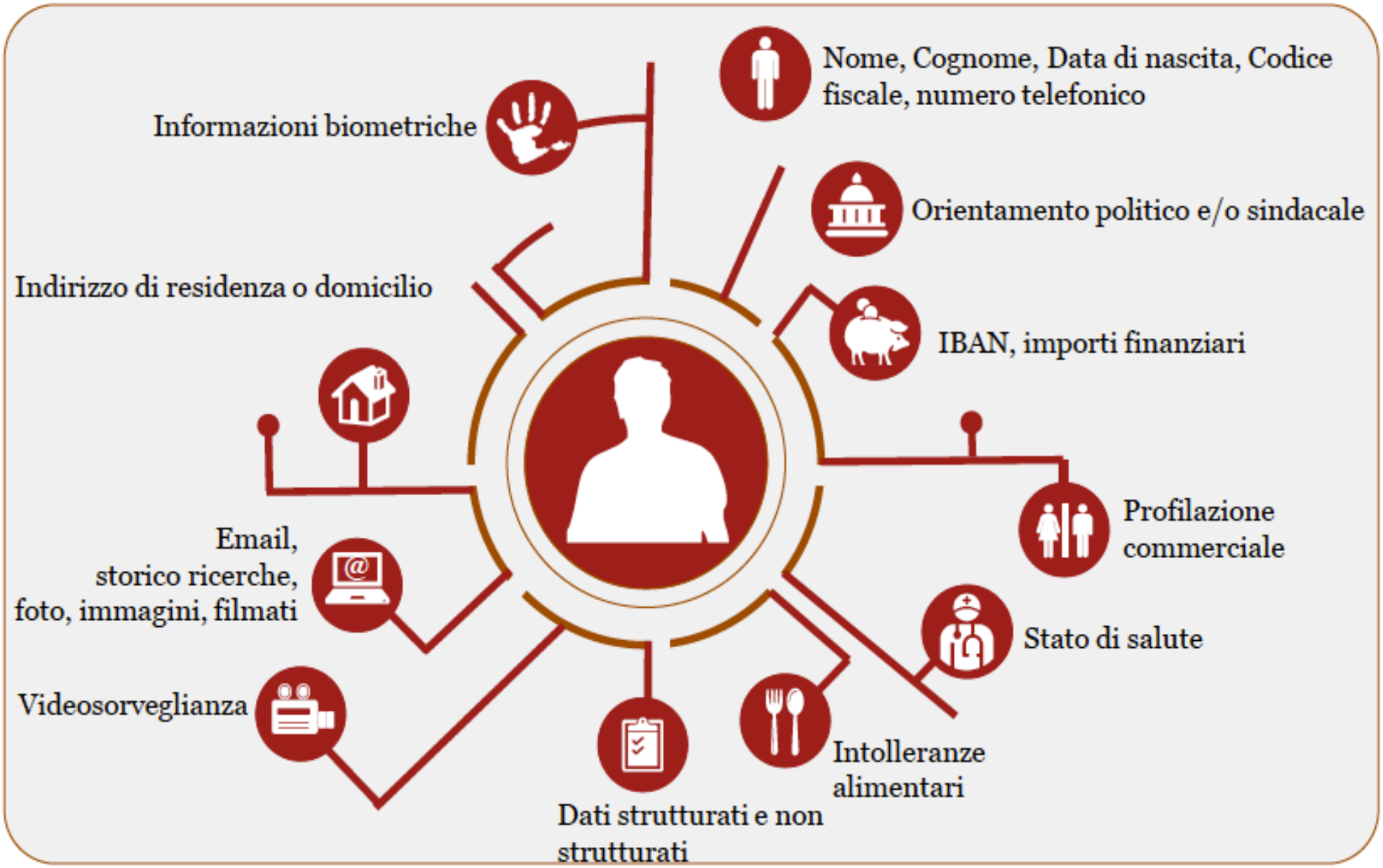
Esempi di dati identificativi...

- nome e cognome
- indirizzo di casa
- indirizzo email
- numero identificativo nazionale
- numero di passaporto
- indirizzo IP (quando collegato ad altri datii)
- numero di targa del veicolo
- numero di patente
- volto, impronte digitali o calligrafia
- numeri di carta di credito
- identità digitale
- data di nascita
- luogo di nascita
- informazioni genetiche
- numero di telefono
- account name o nickname

Dati particolari

[*Art.9 –GDPR*]

l'origine razziale o etnica;
le opinioni politiche;
le convinzioni religiose o filosofiche;
l'appartenenza sindacale;
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.



Dati personali

Regolamento UE 679/2016

Protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla **riservatezza**, **integrità** e **disponibilità** dei dati personali.

Riservatezza dei dati

Gestione della sicurezza in modo tale da mitigare i rischi connessi all'accesso o all'uso delle informazioni in forma non autorizzata.

GDPR

Integrità dei dati

Garanzia che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici.

GDPR

Disponibilità dei dati

Salvaguardia del patrimonio informativo nella garanzia di accesso, usabilità e confidenzialità dei dati.

Da un punto di vista di gestione della sicurezza significa ridurre a livelli accettabili i rischi connessi all'accesso alle informazioni (capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico).

GDPR

Trattamento

[*Art.4 Definizioni –GDPR*]

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

Trattamento dei dati personali

[*Art.5 – GDPR*]

Effettuato nel rispetto dei seguenti principi:

- liceità, correttezza e trasparenza nei confronti dell'interessato;
- limitazione della finalità del trattamento;
- minimizzazione della raccolta dei dati;
- esattezza dei dati rispetto alle finalità per le quali vengono trattati;
- limitazione temporale della conservazione dei dati;
- integrità e riservatezza;
- responsabilizzazione del titolare.

Liceità del trattamento [*Art.6 – GDPR*]

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'**idonea base giuridica**.

Quando il trattamento è lecito?

1. l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

2. 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

3. il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento

4. il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica

5. 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

6. il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento 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 (questo punto non è applicabile però al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti)

GDPR

Il consenso

[*Art.7 – GDPR*]

Deve essere prestato in maniera chiara e semplice, in forma comprensibile e facilmente accessibile.

Il Regolamento non prevede obbligatoriamente la forma scritta per il consenso. Tuttavia considerato che il titolare del trattamento, sempre ai sensi dell'art. 7, par. 1, è onerato di *"dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali"*, è evidentemente raccomandata l'opportunità di provvedere all'acquisizione del consenso in forma scritta.

Deve essere chiaro anche il riconoscimento del diritto a revocare il proprio consenso in qualsiasi momento.

Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutti i requisiti indicati nel Regolamento (UE) 2016/679. In caso contrario è opportuno, prima di tale data, raccogliere nuovamente il consenso degli interessati secondo quanto previsto dalla novella normativa.

Il Regolamento è fondato sul principio della

accountability

Accountability

[artt. 23-25 – *GDPR*]

Adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.

E' il titolare del trattamento ad essere investito del compito (e della responsabilità) di **garantire l'adempimento** agli obblighi previsti dalle norme e l'**efficacia della tutela predisposta.**

Obblighi che comprendono quelli di **riesame ed aggiornamento costante** di tutte le condizioni adottate nel proprio sistema di trattamento e protezione dei dati personali.

GDPR

Responsabilità

Autorizzato al trattamento

Tale figura è colui che effettua materialmente le operazioni di trattamento sui dati personali. Può essere solo una persona fisica e deve agire sotto la diretta autorità del titolare o del responsabile del trattamento.

Informativa

Informativa

[*Art.12-14 – GDPR*]

Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni e le comunicazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

GDPR

Il diritto all'oblio

Diritto all'oblio

[*Art.17 – GDPR*]

Il diritto cosiddetto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata.

Diritto all'oblio

[*Art.17 – GDPR*]

NOVITA' - Il dovere specifico posto a carico del titolare che riceva una richiesta di cancellazione quando i dati che ne sono oggetto siano stati “resi pubblici” dal titolare stesso.

>Il titolare non solo deve cancellare i dati (sempre ovviamente che ritenga la richiesta legittima per quanto lo riguarda), ma deve anche, “tenuto conto della tecnologia disponibile e dei costi di attuazione”, adottare “misure ragionevoli, anche tecniche” per informare della richiesta che gli è pervenuta anche gli altri eventuali titolari che stanno utilizzando i dati a lui resi pubblici (compresi "qualsiasi link, copia o riproduzione")

Portabilità

Portabilità

[*Art.20 – GDPR*]

Un diritto innovativo:

quello di ricevere i dati forniti a un titolare per conservarli in vista di un utilizzo ulteriore, o anche di ottenere la trasmissione degli stessi da un titolare ad un altro “senza impedimenti”.

Privacy “by design” e “by default”

Protezione fin dalla progettazione e per impostazione predefinita

[*Art.25 – GDPR*]

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

GDPR

Protezione fin dalla progettazione e per impostazione predefinita

[*Art.25 – GDPR*]

Ciò implica anche la verifica e l'eventuale necessità di adeguamento degli strumenti (*hardware / software*) attraverso i quali il trattamento viene effettuato (c.d. *"privacy by design"*).

Protezione fin dalla progettazione e per impostazione predefinita

[*Art.25 – GDPR*]

Il titolare del trattamento attua misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ciascuna finalità del trattamento. Obbligo che vale per la quantità dei dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità ai dati stessi (c.d. *"privacy by default"*).

Data breach

Valutazione d'impatto sulla protezione dei dati

Data Protection Officer

(*Responsabile Protezione Dati*)

Registri del trattamento

Sanzioni

Sanzioni

[*Art. 83 – GDPR*]

Il regolamento non fissa un importo specifico per ogni singola violazione, ma solo un massimale.

Sanzioni amministrative pecuniarie (articolo 83 GDPR)

Fino a **€ 20 milioni** o al **4% del fatturato mondiale** totale annuo dell'esercizio precedente, se superiore

In caso di violazione delle disposizioni in materia di, tra le altre:

- ✓ **principi generali** applicabili al trattamento;
- ✓ **condizioni di liceità del trattamento**;
- ✓ trattamento di **categorie particolari di dati**;
- ✓ **diritti dell'interessato**;
- ✓ **trasferimento** dei dati extra UE;
- ✓ norme nazionali in tema di rapporti di lavoro;
- ✓ inosservanza di un ordine da parte dell'autorità di controllo.

Fino a **€ 10 milioni** o al **2% del fatturato mondiale** totale annuo dell'esercizio precedente, se superiore

In caso di violazione delle disposizioni in materia di, tra le altre:

- ✓ trattamento dei dati di minori;
- ✓ *Privacy by Design / Privacy by Default;*
- ✓ mansioni e responsabilità del **responsabile del trattamento;**
- ✓ **registro** delle attività di trattamento;
- ✓ **misure di sicurezza** adeguate;
- ✓ notifica al Garante di una **violazione dei dati personali** e/o comunicazione della stessa agli interessati;
- ✓ **DPIA**;
- ✓ designazione del **DPO** e adempimenti connessi.

GDPR

Condizioni generali per infliggere sanzioni amministrative pecuniarie (art. 83, paragrafo 2, GDPR) Interpretazioni dell'Article 29 Data Protection Working Party			
a	**Natura, gravità e durata** della violazione tenendo in considerazione la natura, oggetto, o finalità del trattamento, nonché il numero di interessati lesi dal danno e il livello del danno subito	**f**	Grado di **cooperazione con il Garante** al fine di porre rimedio alla violazione e attenuare i danni
b	Carattere **doloso o colposo** della violazione	**g**	**Categorie di dati personali** interessate dalla violazione
c	**Misure adottate** dal titolare **per attenuare il danno** subito dagli interessati	**h**	Maniera in cui l'autorità di controllo ha preso conoscenza della violazione e, in particolare, se è stata **notificata** dal titolare
d	Grado di responsabilità del titolare, tenuto conto delle **misure tecniche ed organizzative adottate** ai sensi degli articoli 25 e 32	**i**	Precedente disposizioni di **provvedimenti ex articolo 58, par. 2, GDPR** relativamente allo stesso oggetto e il loro rispetto da parte del titolare
e	**Precedenti violazioni pertinenti** commesse	**j**	Adesione ai **codici di condotta** o ai **meccanismi di certificazione**

Responsabilità civile per danni

[*Art. 82 – GDPR*]

Il titolare si espone innanzitutto ad una responsabilità civile, laddove cagioni un danno per effetto del trattamento dei dati: trattasi di responsabilità di cui all'articolo 2050 c.c., per esercizio di attività pericolosa.

Responsabilità civile per danni

[*Art. 82 – GDPR*]

Chiunque subisca un danno causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno, patrimoniale e non, dal titolare o dal responsabile del trattamento (qualora quest'ultimo non abbia adempiuto agli obblighi specificatamente a lui diretti).
A norma dell'art. 82 Regolamento, l'accusato deve provare la propria innocenza (inversione onere della prova).

Responsabilità civile per danni [*Art. 82 – GDPR*]

I rischi che possono dar luogo a **risarcimento** si configurano se il trattamento:

- cagioni un danno fisico, materiale o immateriale;
- comporti discriminazioni, furto, usurpazione di identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto, decifratura non autorizzata della pseudonimizzazione, diffusioni di dati su origine razziale o etnica, opinioni politiche, convinzioni religiose, appartenenza sindacale, salute, vita sessuale, condanne penali, reati.

Codice Privacy

SANZIONI AMMINISTRATIVE

TITOLO III - Artt. da 166

Art. 166

Presenta due parti:

La prima integra l'apparato sanzionatorio amministrativo introducendo **sanzioni** per la violazione di determinate norme del Codice della privacy.

La seconda parte disciplina il **procedimento amministrativo** per l'applicazione delle sanzioni.

In pratica

A. SANZIONE AMMINISTRATIVA DI CUI ALL'ARTICOLO 83, PARAGRAFO 4, DEL REGOLAMENTO	
Articolo del Codice	**Oggetto**
2-quinquies, comma 2	Informazione ai minori
2-quinquiesdecies,	trattamenti di pubblico interesse a rischio elevato
92, comma 1	Stesura e conservazione cartelle cliniche
93, comma 1	Certificato di assistenza al parto
123, comma 4	Informazioni sui dati relativi al traffico
128	Trasferimento automatico della chiamata
129, comma 2	Elenchi dei contraenti
132-ter	Informazioni sui rischi (servizi di comunicazioni elettronica accessibile al pubblico)
110, comma 1	Ricerca medica, biomedica, epidemiologica; omessa valutazione di impatto; omessa consultazione preventiva del Garante

In pratica

B. SANZIONE AMMINISTRATIVA DI CUI ALL'ARTICOLO 83, PARAGRAFO 5, DEL REGOLAMENTO	
Articolo del Codice	**Oggetto**
2-ter	Base giuridica trattamenti di pubblico interesse/esercizio di pubblici poteri
2-quinquies, comma 1	Consenso del minore
2-sexies	Trattamenti di dati particolari per rilevanti interessi pubblici
2-septies, comma 7	Misure garanzie per dati biometrici
2-octies	Trattamento di dati relativi a condanne e reati
2-terdecies, commi 1, 2, 3 e 4	Dati relativi a persone decedute
52, commi 4 e 5	Diffusione di dati in sentenze
75	Specifiche condizioni in ambito sanitario
78	Informazioni di medico/pediatra

79	Informazioni da parte di strutture pubbliche e private che erogano prestazioni sanitarie e socio-sanitarie
80	Informazioni da parte di altri soggetti
82	Emergenze e tutela della salute e dell'incolumità fisica
92, comma 2	Accesso cartelle cliniche
93, commi 2 e 3	Accesso Certificato di assistenza al parto
96	Trattamento di dati relativi a studenti
99	Durata del trattamento Archiviazione, ricerca, statistica
100, commi 1, 2 e 4	Trattamento dati relativi ad attività di studio e ricerca
101	Archiviazione, ricerca storica Modalità di trattamento)
105 commi 1, 2 e 4	fini statistici o di ricerca scientifica, Modalità di trattamento)
110-bis, commi 2 e 3	Trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici)
111	Regole deontologiche per trattamenti nell'ambito del rapporto di lavoro
111-bis	Informazioni in caso di ricezione di curriculum
116, comma 1	- Istituti di patronato e di assistenza sociale (Conoscibilità di dati su mandato dell'interessato)
120, comma 2	Trattamento dell' L'Istituto per la vigilanza sulle assicurazioni
122	Servizi di comunicazione elettronica Informazioni raccolte nei riguardi del contraente o dell'utente
123, commi 1, 2, 3 e 5	(Dati relativi al traffico)
124	Fatturazione dettagliata
125	Identificazione della linea
126	Dati relativi all'ubicazione)
130, commi da 1 a 5	Comunicazioni indesiderate
131	Informazioni a contraenti e utenti
132	Conservazione di dati di traffico per altre finalità
132-bis, comma 2	Procedure istituite dai fornitori
132-quater	Informazioni sui rischi fornitore di un servizio di comunicazione elettronica
157	Richiesta di informazioni e di esibizione di documenti da parte del garante
2-septies 2-quater.	Violazioni misure di garanzia, delle regole deontologiche e delle modalità tecniche

La norma individua il Garante quale organo competente ad adottare i provvedimenti correttivi e sanzionatori previsti dal GDPR.

SANZIONI PENALI

TITOLO III - Artt. da 167 a 171

Art. 167 (Trattamento illecito di dati)

Punisce diverse condotte consistenti nell'arrecare nocumento all'interessato, in violazione di specifiche previsioni indicate nei primi tre commi dell'articolo

(I)
SOGGETTO ATTIVO: chiunque
CONDOTTA: operare in violazione delle disposizioni in materia di comunicazioni elettroniche
EVENTO: nocumento all'interessato
ELEMENTO SOGGETTIVO: dolo specifico (profitto/danno)
SANZIONE: reclusione da sei mesi a un anno e sei mesi

(II)
SOGGETTO ATTIVO: chiunque
CONDOTTA: trattare dati particolari/condanne/reati in violazione di legge/regolamento/misure di garanzia
EVENTO: nocumento all'interessato
ELEMENTO SOGGETTIVO: dolo specifico (profitto/danno)
SANZIONE: reclusione da uno a tre anni

(III)
SOGGETTO ATTIVO: chiunque
CONDOTTA: trasferimento dati verso paese terzo od organizzazione internazionale in violazione GDPR
EVENTO: nocumento all'interessato
ELEMENTO SOGGETTIVO: dolo specifico (profitto/danno)
SANZIONE: reclusione da uno a tre anni

Art. 167-bis

(Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala).

E' stata introdotta la "**Comunicazione e diffusione illecita** di dati personali oggetto di trattamento **su larga scala**".

È punita la comunicazione o diffusione di un **archivio automatizzato** o di una parte sostanziale di esso, senza consenso quando è stabilito per la liceità del trattamento, al fine di trarne profitto o di arrecare un danno.

In pratica

(I)
SOGGETTO ATTIVO: chiunque CONDOTTA: in violazione di legge / regolamento, comunicare o diffondere un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala ELEMENTO SOGGETTIVO: dolo specifico (profitto / danno) SANZIONE: reclusione da uno a sei anni.

(II)
SOGGETTO ATTIVO: chiunque CONDOTTA: comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione ELEMENTO SOGGETTIVO: dolo specifico (profitto / danno) SANZIONE: reclusione da uno a sei

Art. 167-ter

(Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala).

Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è punito con la **reclusione da uno a quattro anni**.

In pratica

(I)
SOGGETTO ATTIVO: chiunque
CONDOTTA: acquisire con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala
ELEMENTO SOGGETTIVO: dolo specifico (profitto/danno)
SANZIONE: reclusione da uno a quattro anni

Art. 168

(Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante).

Sancisce la punibilità, con la reclusione da **sei mesi a tre anni**, dei soggetti che, nei procedimenti davanti al Garante, dichiarano o attestano il falso.

Reclusione **fino ad un anno** a carico di chi cagiona intenzionalmente una interruzione o turba la regolarità dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante.

In pratica

(I)
SOGGETTO ATTIVO: chiunque
CONDOTTA: in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiarare o attestare falsamente notizie o circostanze o produrre atti o documenti falsi
ELEMENTO SOGGETTIVO: dolo
SANZIONE: da sei mesi a tre anni

(II)
SOGGETTO ATTIVO: chiunque
CONDOTTA: cagionare un'interruzione o turbare la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti
ELEMENTO SOGGETTIVO: dolo intenzionale
SANZIONE: reclusione sino ad un anno

Art. 170

(Inosservanza di provvedimenti del Garante)

Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 58, paragrafo 2, lettera f) del Regolamento, dell'articolo 2-septies, comma 1, nonché i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'articolo 13 della legge 25 ottobre 2017, n. 163 è punito con la **reclusione da tre mesi a due anni**.

In pratica

(I)
SOGGETTO ATTIVO: chiunque, essendovi tenuto
CONDOTTA: Inosservanza di provvedimenti del Garante
ELEMENTO SOGGETTIVO: dolo
SANZIONE: da tre mesi a due anni

Art. 171

(Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori)

La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, è punita con le **sanzioni di cui all'articolo 38** della medesima legge.

In pratica

(I)
SOGGETTO ATTIVO: datore di lavoro
CONDOTTA: violazione obbligo di accordo sindacale/autorizzazione amministrativa per installare sistemi di controllo indiretto; violazione divieto di indagine sulla opinione dei lavoratori
ELEMENTO SOGGETTIVO: dolo
SANZIONE: da lire 300.000 a lire 3.000.000 o con l'arresto da 15 giorni ad un anno.
Nei casi più gravi le pene dell'arresto e dell'ammenda sono applicate congiuntamente.
Quando per le condizioni economiche del reo, l'ammenda stabilita nel primo comma può presumersi inefficace anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo.
Nei casi più gravi, l'autorità giudiziaria ordina la pubblicazione della sentenza penale di condanna.

Esempio di sanzione

Il Garante per la privacy ha comminato sanzioni di **4000 euro** ciascuna a due Licei della regione Campania per aver diffuso illecitamente informazioni non necessarie e dati sulla salute nelle graduatorie dei docenti pubblicate sui siti web degli istituti. [doc. web. nn. 9283029 e 9283014]

Esempio di sanzione

Con la sentenza n. 246/2019 la Corte dei Conti- Sezione Giurisdizionale per il Lazio – ha ritenuto responsabile il Dirigente scolastico per il danno indiretto causato all'Istituto, a seguito del pagamento di una sanzione amministrativa, irrogata dal Garante della privacy per la pubblicazione su internet di una circolare contente dati riguardanti scolari affetti da disabilità.

Nella vicenda in esame l'Autorità Garante per la Protezione dei dati Personali veniva adita dal genitore di un alunno disabile, il cui nominativo era stato divulgato in rete.

L'Autorità, stante la diffusione su internet dati idonei a rilevare lo stato di salute di minori di età, in violazione del Codice in materia di protezione dei dati Personali, irrogava all'Istituto scolastico la sanzione amministrativa di **€ 20.000,00.**

Tale sanzione veniva pagata con i fondi della scuola, con conseguente danno al bilancio dell'Istituto, le cui casse risultavano quindi depauperate ad opera della condotta gravemente negligente del Dirigente scolastico.

Dal giudizio era infatti emerso che il Dirigente scolastico aveva adottato la circolare interna avente per oggetto la "Convocazione GHL (Gruppo di Lavoro per l'Handicap operativo)", nella quale era contenuto un elenco dei nomi degli scolari minori dell'Istituto affetti da disabilità.

Esempio di sanzione

Diffusione, mediante affissione sulla porta di ingresso della scuola dell'infanzia di Otranto, alcuni elenchi contenenti dati personali di soggetti minorenni (nomi di minori, date di nascita, indirizzi di residenza, numeri di telefono e la dicitura "manca copia vaccini).

Tale diffusione è avvenuta in violazione della normativa a tutela dei dati personali e, specificamente:

a) in violazione dei principi di "liceità, correttezza e trasparenza" e di "minimizzazione dei dati", di cui all'art. 5, par. 1, lett. a) e c) del Regolamento;

b) in assenza di un idoneo presupposto normativo per la pubblicazione dei predetti dati personali, in violazione dell'art. 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del Regolamento e 2-ter, commi 1 e 3, del Codice.

Sanzione: **2000 €**

La soluzione...

1. Misure tecniche e organizzative che realizzano la compliance normativa e contrastano le minacce alla sicurezza prevenendo i rischi ad esse correlate.

2. Figure professionali adeguate (es. DPO, consulente privacy).

3. Consapevolezza (sensibilizzazione e formazione).

Come trattare correttamente i dati
https://www.garanteprivacy.it/home/doveri

GDPR

ing. Alberto Bulzatti
Mob. 338 5442434
studiobulzatti@gmail.com