



NICOLA FABIANO #4228



Il trattamento dei dati personali Regolamento UE 2016/679 (GDPR)

Avv. Nicola Fabiano



Chi sono

- Avvocato, Cassazionista, Specialista in Diritto Civile, Ricercatore indipendente;
- Membro del Gruppo di Lavoro della **FIIF** (Fondazione Italiana per l'Innovazione Forense) del **CNF** (Consiglio Nazionale Forense);
- Vincitore del corso promosso dal **Consiglio d'Europa** in collaborazione con il Consiglio Nazionale Forense (**CNF**) su “*Data Protection and Privacy Rights*”;
- Consulente del Governo della Repubblica di San Marino per la redazione della normativa in materia di protezione dei dati personali
- Certificato:
 - ➔ ***ICT Security Manager UNI 11506:2013***
 - ➔ ***Responsabile della Protezione dei Dati (RPD/DPO) UNI 11697:2017***
 - ➔ ***Professionista dei sistemi di gestione della sicurezza delle informazioni ISO 27021:2017***
- Academic Member of the Athens Institute for Education and Research (ATINER), belonging to the Law Research Unit and the Computer Research Unit, 2017;
- Iscritto nella lista europea degli esperti in Societal Security;
- Relatore a conferenze internazionali;
- Vincitore di numerosi Awards

Temi da trattare

- ☑ Regolamento Generale sulla Protezione dei Dati (GDPR) - Reg. UE 2016/679
- ☑ Profili soggettivi
 - ➡ Il titolare del trattamento (art. 24 GDPR)
 - ➡ I contitolari (art. 27 GDPR)
 - ➡ Il responsabile del trattamento (art. 28 GDPR)
 - ➡ Le persone autorizzate (art. 4 - art. 29 GDPR)
 - ➡ Il Responsabile della Protezione dei Dati - RPD/DPO (artt. 37-39 GDPR)
- ☑ Principi al trattamento dei dati (art. 5 GDPR)
- ☑ Liceità del trattamento (art. 6 GDPR)
- ☑ I dati personali
 - ➡ categorie particolari di dati (art. 9 GDPR)
 - ➡ dati personali relativi a condanne penali e reati (art. 10 GDPR)
- ☑ Il trattamento dei dati personali (art. 4- art. 5 GDPR)
- ☑ Data protection by design and by default (art. 25 GDPR)
- ☑ Il trasferimento dei dati personali verso paesi terzi o organizzazioni internazionali (artt. 44-50 GDPR)
- ☑ Sicurezza del trattamento (art. 32)
- ☑ Le responsabilità (art. 82 GDPR)
- ☑ Le sanzioni (art. 83 GDPR)

Le principali fonti normative

- CARTA DEI DIRITTI FONDAMENTALI DELL'UNIONE EUROPEA (2017/C 202/02) - Artt. 7-8
- Trattato sul funzionamento dell'UE (TFUE) - Art. 16, § 1
- Decreto Legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”
- 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) - **applicabile dal 25/5/2018**
- Direttiva 2002/58/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)
- Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche)

Convenzioni

- Convenzione europea dei diritti dell'uomo (CEDU) - Art. 8
- Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione 108/1981)

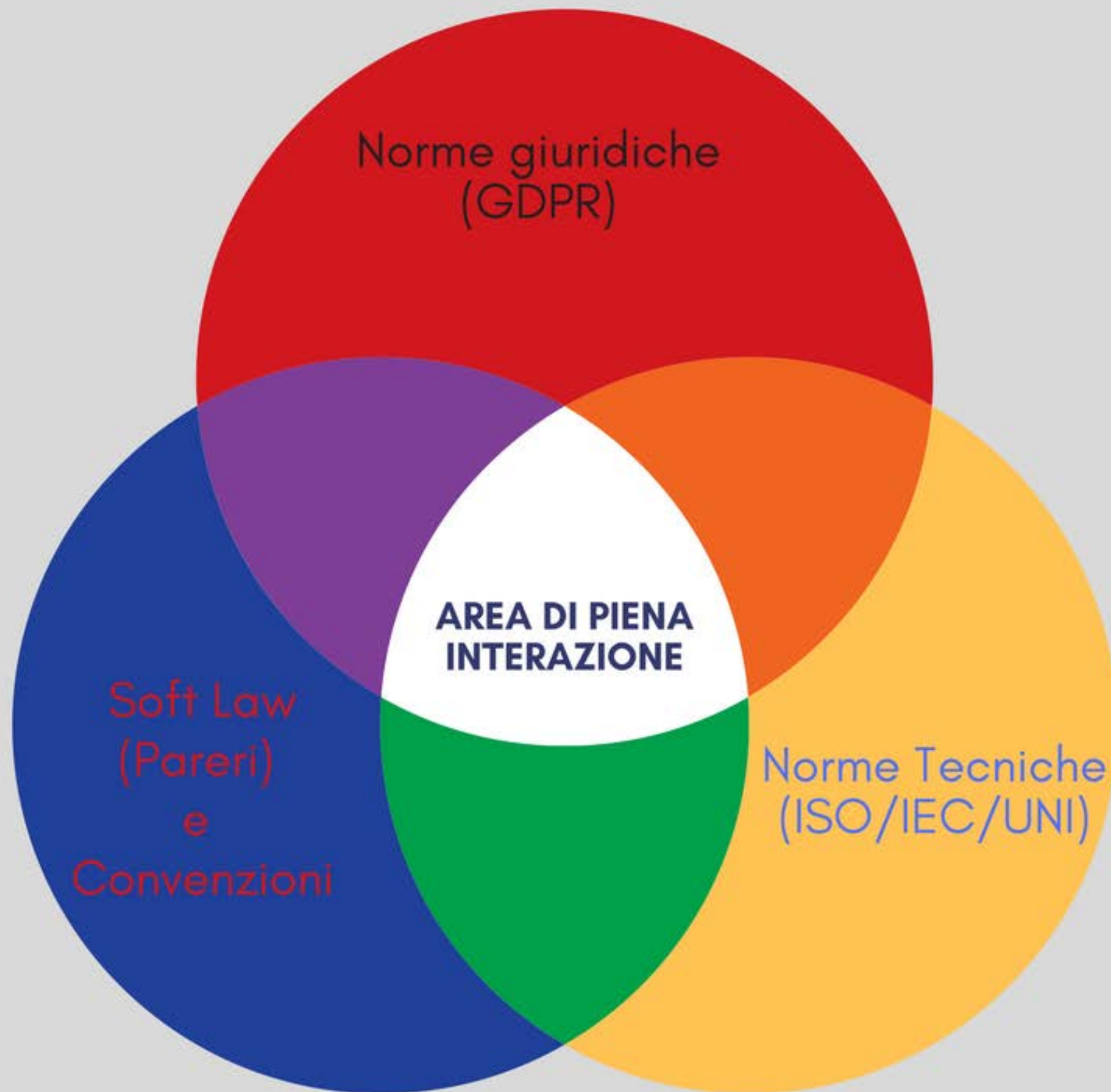
Soft Law

- ☑ Provedimenti del Garante per la protezione dei dati personali
- ☑ Opinions (Pareri) Art. 29WP (EDPB)
- ☑ Raccomandazioni, risoluzioni e decisioni degli Organi statutari del Consiglio d'Europa (Assemblea parlamentare e Consiglio dei Ministri)
- ☑ Pareri e studi della Commissione europea per la Democrazia attraverso il Diritto (Commissione di Venezia) - Organo consultivo del Consiglio d'Europa in materia costituzionale

Principali norme tecniche

- ☑ ISO/IEC 27000:2016 - **SGSI** (Panoramica e vocabolario)
- ☑ ISO/IEC 27001:2013 - **SGSI** (Requisiti)
- ☑ ISO/IEC 27002:2014 - **SGSI** (Codice di condotta per i controlli di sicurezza delle informazioni)
- ☑ ISO/IEC 19011:2011 (Linee guida per audit di sistemi di gestione)

-
- International Electrotechnical Commission (IEC)
 - International Organization for Standardization (ISO)
 - Ente Nazionale Italiano di Unificazione (UNI)



Carta dei Diritti Fondamentali dell'Unione Europea

Articolo 7

Rispetto della vita privata e della vita familiare

Ogni persona **ha diritto al rispetto** della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni.

Articolo 8

Protezione dei dati di carattere personale

1. Ogni persona **ha diritto alla protezione dei dati di carattere personale che la riguardano.**
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Le limitazioni

Tali diritti sono soggetti a limitazione ai sensi dell'art. 52.1 della
CEDU

Articolo 52

Portata e interpretazione dei diritti e dei principi

1. **Eventuali limitazioni** all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta **devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà.** Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

Le limitazioni

Nella causa Volker und Markus Schecke, la CGUE era stata chiamata a valutare la proporzionalità della pubblicazione, imposta dal diritto dell'Unione, dei nominativi dei beneficiari di stanziamenti UE per l'agricoltura e degli importi da questi percepiti. La CGUE, dopo aver rammentato che il diritto alla protezione dei dati non ha carattere assoluto, ha ritenuto che la pubblicazione su un sito web dei nominativi dei beneficiari di due fondi agricoli UE e degli importi precisi da questi percepiti **costituisse un'ingerenza nella loro vita privata**, in generale, e **nella protezione dei loro dati personali, in particolare**.

La CGUE ha ritenuto che tale ingerenza nell'esercizio dei diritti sanciti agli articoli 7 e 8 della Carta fosse prevista dalla legge e rispondesse a una finalità di interesse generale riconosciuta dall'Unione europea, ossia rafforzare la trasparenza sull'uso dei fondi europei.

Tuttavia, la CGUE ha concluso che la pubblicazione dei nominativi di persone fisiche beneficiarie di stanziamenti agricoli UE da parte dei due fondi e dei precisi importi da questi percepiti costituisse una misura non proporzionata e non giustificabile ai sensi dell'articolo 52.1 della Carta.

La Corte ha pertanto dichiarato la parziale invalidità delle disposizioni del diritto dell'Unione in materia di pubblicazione di informazioni pertinenti ai beneficiari di fondi europei per l'agricoltura.

Trattato sul funzionamento dell'Unione Europea (TFUE)

Articolo 16

(ex articolo 286 del TCE)

1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.
Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea.

Convenzione europea dei diritti dell'uomo (CEDU)

ARTICOLO 8

Diritto al rispetto della vita privata e familiare

1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.
2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

Convenzione 108/1981

Articolo 1 – Oggetto e scopo

Scopo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo **diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano («protezione dei dati»).**

GDPR e Direttiva 2002/58/CE

Articolo 95

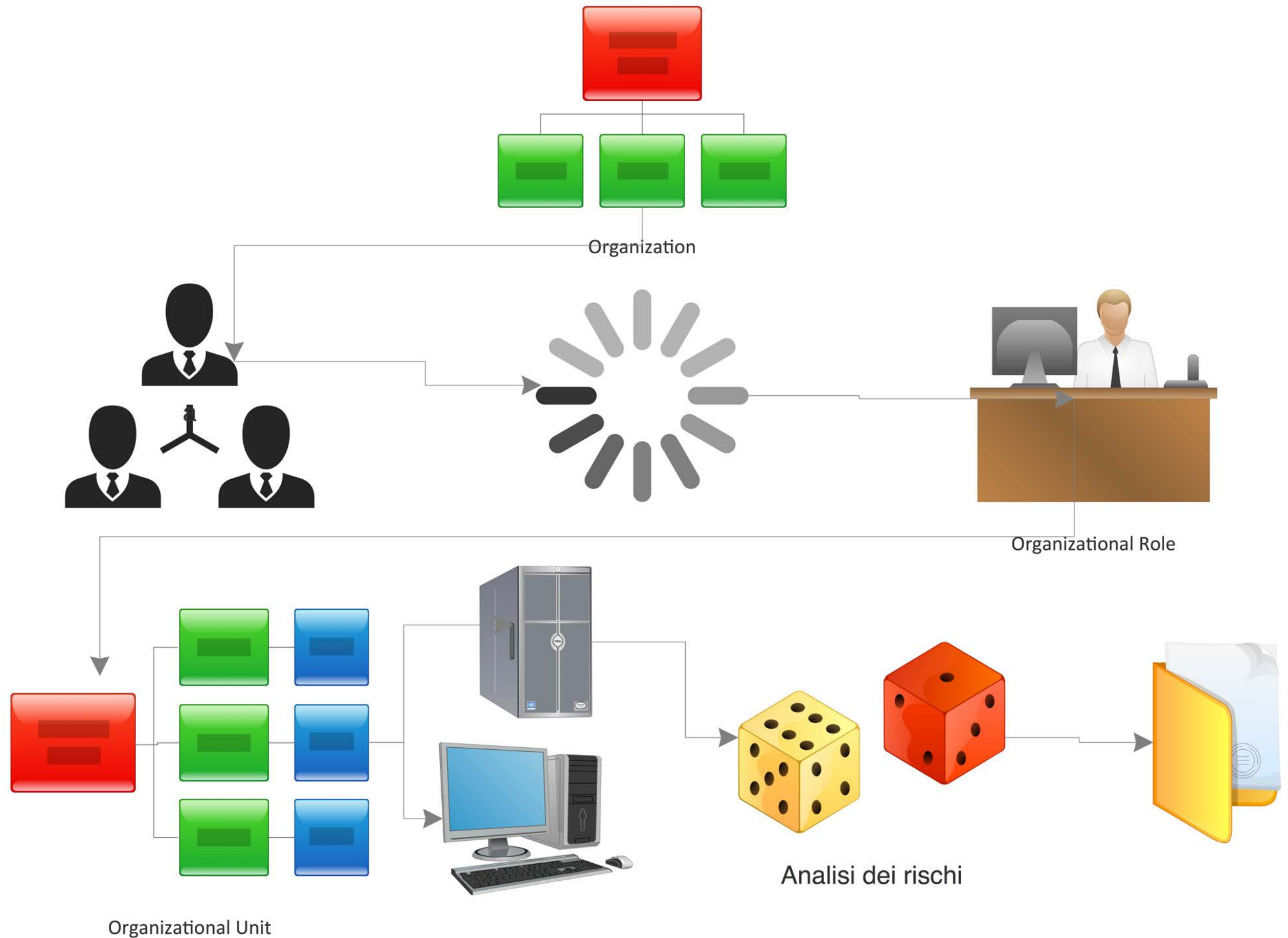
Rapporto con la direttiva 2002/58/CE

Il presente regolamento non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva 2002/58/CE.

La struttura del GDPR

- ☑ CAPO I - **Disposizioni generali** (artt. 1-4)
- ☑ CAPO II - **Principi** (artt. 5-11)
- ☑ CAPO III - **Diritti dell'interessato** (artt. 12-23)
- ☑ CAPO IV - **Titolare del trattamento e responsabile del trattamento** (artt. 24-43)
- ☑ CAPO V - Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali (artt. 44-50)
- ☑ CAPO VI - Autorità di controllo indipendenti (artt. 51-59)
- ☑ CAPO VII - Cooperazione e coerenza (artt. 60-76)
- ☑ CAPO VIII - **Mezzi di ricorso, responsabilità e sanzioni** (artt. 77-84)
- ☑ CAPO IX - Disposizioni relative a specifiche situazioni di trattamento (artt. 85-91)
- ☑ CAPO X - Atti delegati e atti di esecuzione (artt. 92-93)
- ☑ CAPO XI - Disposizioni finali (artt. 94-99)

GDPR Assessment



Il dato personale

Il dato personale

Art. 4 - Definizioni

1) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («**interessato**»); 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; (**C26, C27, C30**)

Profili soggettivi

Profili soggettivi

Art. 4 - Definizioni

- «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («**interessato**»);
- «**titolare del trattamento**»: 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 di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- «**rappresentante**»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
- «**impresa**»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
- «**gruppo imprenditoriale**»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

CAPO IV

Titolare del trattamento e responsabile del trattamento

Il titolare del trattamento

Sezione 1 Obblighi generali

Articolo 24

Responsabilità del titolare del trattamento (C74-C78)

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, 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.
2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.
3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Contitolari del trattamento

Articolo 26

Contitolari del trattamento (C79)

1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.
2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
3. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

Responsabile del trattamento 1/4

Articolo 28

Responsabile del trattamento (C81)

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

Responsabile del trattamento 2/4

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

- a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- c) adotti tutte le misure richieste ai sensi dell'articolo 32;
- d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
- e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
- f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e
- h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Responsabile del trattamento 3/4

4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.
5. L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.
6. Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43.

Responsabile del trattamento 4/4

7. La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.
8. Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63.
9. Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.
10. Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.

Persone autorizzate

«**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e **le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;**

Articolo 29

Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Registri delle attività di trattamento

Articolo 30

Registri delle attività di trattamento

1. Ogni **titolare del trattamento** e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
 - a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
 - b) le finalità del trattamento;
 - c) una descrizione delle categorie di interessati e delle categorie di dati personali;
 - d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
 - e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
 - f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
 - g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
2. Ogni **responsabile del trattamento** e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:
 - a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
 - b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
 - c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
 - d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
3. **I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.**
4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento **mettono il registro a disposizione dell'autorità di controllo.**
5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, **a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.**

Il trattamento dei dati personali

Definizione di “trattamento”

2) «**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 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;

I Principi nel GDPR

Avv. Nicola Fabiano

Principi

Articolo 5

Principi applicabili al trattamento di dati personali

<p>1. applicazione dei principi di liceità, correttezza e trasparenza (art. 5.1a, GDPR);</p> <p>2. dati raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità (art. 5.1b, GDPR);</p> <p>3. minimizzazione dei dati (5.1c);</p> <p>4. dati esatti e se necessario aggiornati (5.1d);</p> <p>5. dati conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (art. 5.1e, GDPR);</p> <p>6. dati trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principi di integrità e riservatezza) [art. 5.1f GDPR];</p>	<p>1. I dati personali sono:</p> <p>a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);</p> <p>b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);</p> <p>c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);</p> <p>d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);</p> <p>e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);</p> <p>f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).</p>
---	---

I Principi

Articolo 5

Principi applicabili al trattamento di dati personali

- a) «liceità, correttezza e trasparenza»
- b) «limitazione della finalità»
- c) «minimizzazione dei dati»
- d) «esattezza»
- e) «limitazione della conservazione»
- f) «integrità e riservatezza»

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di provarlo («responsabilizzazione»).

L'informativa

L'informativa - Art. 13

Articolo 13 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

- a) **l'identità e i dati di contatto** del titolare del trattamento e, ove applicabile, del suo rappresentante;
- b) **i dati di contatto** del responsabile della protezione dei dati, ove applicabile;
- c) **le finalità del trattamento** cui sono destinati i dati personali nonché la base giuridica del trattamento;
- d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- e) **gli eventuali destinatari** o le eventuali categorie di destinatari dei dati personali;
- f) 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 o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

- a) **il periodo di conservazione dei dati personali** oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- b) **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;
- c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), **l'esistenza del diritto di revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- d) **il diritto di proporre reclamo** a un'autorità di controllo;
- e) **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;
- f) **l'esistenza di un processo decisionale automatizzato, compresa la profilazione** di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

L'informativa - Art. 14

Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

1. Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni:

- a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
- c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- d) le categorie di dati personali in questione;
- e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

2. Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:

- a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- c) 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 dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
- e) il diritto di proporre reclamo a un'autorità di controllo;
- f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
- g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

3. Il titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2:

- a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
- b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure
- c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

Il consenso

Consenso

Principali norme sul consenso

Art. 4, par. 1 n. 11 - Definizioni

«**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Articolo 6 , par. 1 lett. a) - Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità

Articolo 7 - Condizioni per il consenso

1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

Articolo 8 - Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione

1. Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

1. **consenso esplicito**: l'onere della prova sulla corretta acquisizione del consenso e della liceità del trattamento graverà sul responsabile dello stesso (art. 7 GDPR);
2. **necessità del consenso esplicito** per l'offerta diretta di servizi della società dell'informazione ai minori che abbiano compiuto gli anni 16; ove il minore abbia **un'età inferiore ai 16 anni**, tale trattamento è lecito soltanto se e nella misura in cui **tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale** (art. 8 GDPR).
3. **necessità del consenso esplicito** per il trattamento di **dati personali (categorie particolari di dati personali) che rivelino** l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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 (art. 9 GDPR);
4. il consenso esplicito può essere **revocato** in qualsiasi momento (art. 13 GDPR);
5. **necessità del consenso esplicito** dell'interessato per essere sottoposto a una **decisione basata unicamente sul trattamento automatizzato, compresa la profilazione**, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona (art. 20 GDPR).

Il consenso 2/2

forma del consenso

Regolamento UE 679/2016

Articolo 7 - Condizioni per il consenso

1. Qualora il trattamento **sia basato sul consenso**, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
2. 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. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3. 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.
4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Il consenso dei minori

Regolamento UE 679/2016

Articolo 8

Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione

1. Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore **è lecito ove il minore abbia almeno 16 anni**. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.
Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.
2. Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.
3. Il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore.

Diritto alla cancellazione (oblio)

Diritto all'oblio 1/2

Regolamento UE 679/2016

Articolo 17

Diritto alla cancellazione («diritto all'oblio»)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, **se sussiste** uno dei motivi seguenti:

- a) i dati personali **non sono più necessari** rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- b) l'interessato **revoca il consenso** su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
- c) l'interessato **si oppone al trattamento** ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
- d) i dati personali sono stati **trattati illecitamente**;
- e) i dati personali devono essere cancellati **per adempiere un obbligo legale** previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- f) i dati personali **sono stati raccolti** relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1 (NDR minori di 16 anni).

Diritto all'oblio 2/2

Regolamento UE 679/2016

Articolo 17

Diritto alla cancellazione («diritto all'oblio»)

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato **di cancellare** qualsiasi link, copia o riproduzione dei suoi dati personali.

3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:

- a) per **l'esercizio del diritto alla libertà di espressione e di informazione**;
- b) per **l'adempimento di un obbligo legale** che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- c) per **motivi di interesse pubblico** nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
- d) a fini di **archiviazione** nel pubblico interesse, di **ricerca scientifica o storica o a fini statistici** conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
- e) per l'accertamento, l'esercizio o la difesa di un diritto **in sede giudiziaria**.

La sicurezza

La sicurezza

Regolamento UE 679/2016

Articolo 32 - Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, 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:

- a) la pseudonimizzazione e la cifratura dei dati personali;
- b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, **si tiene conto in special modo dei rischi** presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

**Protezione dei dati fin dalla progettazione
e per impostazione predefinita**

Data protection by design and by default

Data protection by design and by default

Regolamento UE 679/2016

Articolo 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la **pseudonimizzazione**, volte ad attuare in modo efficace i principi di protezione dei dati, quali la **minimizzazione**, e a **integrare nel trattamento le necessarie garanzie** al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
2. Il titolare del trattamento mette in atto **misure tecniche e organizzative adeguate** per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. **Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.** In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

Notifica di una violazione dei dati personali all'autorità di controllo

Data breach notification

Violazione dei dati personali

«**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

Violazione dei dati personali

Regolamento UE 679/2016

Articolo 33 - Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento **notifica la violazione all'autorità di controllo competente** a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, **entro 72 ore** dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. **Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.**
3. La notifica di cui al paragrafo 1 deve almeno:
 - a) **descrivere la natura della violazione** dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
 - b) **comunicare il nome e i dati di contatto** del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
 - c) **descrivere le probabili conseguenze** della violazione dei dati personali;
 - d) **descrivere le misure adottate** o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Il titolare del trattamento **documenta qualsiasi violazione dei dati personali**, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Valutazione di impatto sulla protezione dei dati personali

Data Protection Impact Assessment

Valutazione d'impatto (DPIA)

Regolamento UE 679/2016

Articolo 35

Valutazione d'impatto sulla protezione dei dati

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
2. Il titolare del trattamento, allorché svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.
3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:
 - a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
 - b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
 - c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Responsabile della protezione dei dati

Data Protection Officer

Responsabile della protezione dei dati (DPO)

Regolamento UE 679/2016

Articolo 37

Designazione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:
 - a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
 - b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
 - c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.
2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.
3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.
4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.
5. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.
6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.
7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

II DPO

Articolo 38

Posizione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.
4. Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.
6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

II DPO

Articolo 39

Compiti del responsabile della protezione dei dati

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:
 - a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
 - b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
 - c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
 - d) cooperare con l'autorità di controllo; e
 - e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

**Trasferimenti di dati personali
verso
paesi terzi o organizzazioni internazionali**

Qual è l'incidenza territoriale del GDPR ?

Incidenza territoriale del GDPR



Ambito di applicazione territoriale del GDPR

Articolo 3

Ambito di applicazione territoriale

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

Il concetto di stabilimento

Articolo 4

Definizioni

«**stabilimento principale**»: (C36, C37)

- a) per quanto riguarda un **titolare del trattamento** con stabilimenti in più di uno Stato membro, **il luogo della sua amministrazione centrale** nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che **quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni**, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo **stabilimento principale**;
- b) con riferimento a un **responsabile del trattamento** con stabilimenti in più di uno Stato membro, **il luogo in cui ha sede la sua amministrazione centrale nell'Unione** o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione **in cui sono condotte le principali attività di trattamento** nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

**Trasferimenti di dati personali
verso
paesi terzi o organizzazioni internazionali**

Disciplina nel GDPR

Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali

CAPO V

- **Articolo 44** - *Principio generale per il trasferimento (C101, C102)*
- **Articolo 45** - *Trasferimento sulla base di una decisione di adeguatezza (C103, C107, C167-C169)*
- **Articolo 46** - *Trasferimento soggetto a garanzie adeguate (C108, C109, C114)*
- **Articolo 47** - *Norme vincolanti d'impresa (C110, C167-C168)*
- **Articolo 48** - *Trasferimento o comunicazione non autorizzati dal diritto dell'Unione (C115)*
- **Articolo 49** - *Deroghe in specifiche situazioni (C111-C114)*
- **Articolo 50** - *Cooperazione internazionale per la protezione dei dati personali (C116)*

?

Principi generali

Ambito soggettivo

- **Paesi terzi (non EU)**
- **«organizzazione internazionale»**: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati (art. 4)

Direttiva 2014/23/UE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 26 febbraio 2014 sull'aggiudicazione dei contratti di concessione

Articolo 6 § 4

Per «organismi di diritto pubblico» si intendono gli organismi che presentano tutte le seguenti caratteristiche:

- a) sono istituiti per lo specifico scopo di soddisfare esigenze di interesse generale, aventi carattere non industriale o commerciale;
- b) sono dotati di personalità giuridica; e
- c) sono finanziati in modo maggioritario dallo Stato, dalle autorità regionali o locali o da altri organismi di diritto pubblico; o la cui gestione è posta sotto la vigilanza di tali autorità o organismi; o il cui organo di amministrazione, di direzione o di vigilanza è costituito da membri più della metà dei quali è designata dallo Stato, dalle autorità regionali o locali o da altri organismi di diritto pubblico.

Direttiva 2014/24/UE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 26 febbraio 2014 sugli appalti pubblici e che abroga la direttiva 2004/18/CE

Articolo 2 § 1

4) «organismi di diritto pubblico»: gli organismi che hanno tutte le seguenti caratteristiche:

- a) sono istituiti per soddisfare specificatamente esigenze di interesse generale, aventi carattere non industriale o commerciale;
- b) sono dotati di personalità giuridica; e
- c) sono finanziati per la maggior parte dallo Stato, dalle autorità regionali o locali o da altri organismi di diritto pubblico; o la loro gestione è posta sotto la vigilanza di tali autorità o organismi; o il loro organo di amministrazione, di direzione o di vigilanza è costituito da membri più della metà dei quali è designata dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico.

Direttiva 2014/25/UE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 26 febbraio 2014 sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali e che abroga la direttiva 2004/17/CE

Articolo 3 § 4

Per «organismi di diritto pubblico» si intendono gli organismi che hanno tutte le seguenti caratteristiche:

- a) sono istituiti per soddisfare specificatamente esigenze di interesse generale, aventi carattere non industriale o commerciale;
- b) sono dotati di personalità giuridica; e
- c) sono finanziati per la maggior parte dallo Stato, dalle autorità regionali o locali o da altri organismi di diritto pubblico; o la loro gestione è posta sotto la vigilanza di tali autorità o organismi; o il loro organo di amministrazione, di direzione o di vigilanza è costituito da membri più della metà dei quali è designata dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico.

Principi generali

Articolo 44

Principio generale per il trasferimento

Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo **soltanto se** il **titolare del trattamento e il responsabile del trattamento** rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. **Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato.**

Analisi	
Unica condizione:	soltanto se
Ambito soggettivo:	Titolare e responsabile
Ambito oggettivo:	Rispetto delle condizioni
Finalità:	Assicurare il livello di protezione

Condizioni per il trasferimento ai sensi del GDPR

1. Decisione di adeguatezza
2. Trasferimento soggetto a garanzie adeguate
3. Norme vincolanti di impresa (BCR)
4. Deroghe in specifiche situazioni

Schema sulla decisione di adeguatezza

Prima fase (valutazione - § § 1 e 2)

- 1. **Competenza:** Commissione Europea
- 1. **Giudizio:** insindacabile della Commissione Europea
- 1. **Oggetto del giudizio:** garanzia di un livello di protezione adeguata
- 2. **Elementi di valutazione:**
 - a) lo stato di diritto
 - b) l'esistenza e l'effettivo funzionamento di un'Autorità
 - c) gli impegni internazionali assunti

Seconda fase (emissione dell'atto di esecuzione - § 3)

- 3. **Durata dell'atto di esecuzione:** temporanea di 4 anni (riesame periodico)
- 3. **Contenuto dell'atto di esecuzione:** specifica l'ambito di applicazione geografico e settoriale e, ove possibile, identifica la o le autorità di controllo (§ 2, lett. b)
- 3. **Modalità di adozione dell'atto di esecuzione:** procedura d'esame ex art. 93, § 2

Terza fase (controllo § 4)

- 4. **Poteri della Commissione:** controllo su base continuativa
- 4. **Ambito del controllo:** decisioni adottate ai sensi del § 3 e dell'art. 25, § 6, della Direttiva 95/46/CE

Quarta fase (esito del controllo § § 5 - 6 - 7)

- 5. **Possibile esito del riesame:** revoca, modifica o sospensione della decisione di adeguatezza senza effetto retroattivo (impregiudicati i trasferimenti ex § 7)
- 5. **Modalità:** procedura ex art. 93, § 2 o in casi di urgenza ex art. 93, § 2
- 6. **Soluzioni:** consultazioni con il paese terzo o l'organizzazione internazionale per porre rimedio

Quinta fase (pubblicità § 8)

- 8. **Pubblicità:** Gazzetta Ufficiale dell'Unione europea e sito web Commissione EU

Decisioni precedenti (§ 9)

- 9. **Sorte delle decisioni in base alla Direttiva 95/46/CE:** in vigore fino a modifica, sostituzione o abrogazione

Trasferimento soggetto a garanzie adeguate

Trasferimento soggetto a garanzie adeguate

Condizioni (art. 46, § 1)

Presupposti: mancanza di una decisione di adeguatezza

Trasferimento ammesso solo in presenza di garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

— — —

Soluzione 1: garanzie adeguate (art. 46, § 2)

- a) uno **strumento giuridicamente vincolante e avente efficacia esecutiva** tra autorità pubbliche o organismi pubblici
- b) le **norme vincolanti d'impresa**
- c) le **clausole tipo di protezione dei dati adottate dalla Commissione**
- d) le **clausole tipo di protezione dei dati adottate da un'autorità di controllo** e approvate dalla Commissione
- e) un **codice di condotta approvato a norma dell'articolo 40**, unitamente all'**impegno vincolante ed esecutivo** da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; o
- f) un **meccanismo di certificazione approvato a norma dell'articolo 42**, unitamente all'**impegno vincolante ed esigibile** da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.

— — —

Soluzione 2: ulteriori garanzie adeguate (art. 46, § 3) con autorizzazione dell'autorità di controllo

- a) le **clausole contrattuali** tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale; o
- b) le **disposizioni da inserire in accordi amministrativi** tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati.

Meccanismo di coerenza (art. 46, § 4)

L'autorità di controllo applica il meccanismo di coerenza ex articolo 63.

Autorizzazioni precedenti (§ 5)

9. Autorizzazioni precedenti in base alla Direttiva 95/46/CE: in vigore fino a modifica, sostituzione o abrogazione

Trasferimento soggetto a garanzie adeguate

Sito web della Commissione Europea

Adequacy of the protection of personal data in non-EU countries

Trasferimenti EU-USA

Safe Harbour

CGUE - SENTENZA DELLA CORTE (Grande Sezione), 6 ottobre 2015, causa C-362/14, avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dalla High Court (Corte d'appello, Irlanda), con decisione del 17 luglio 2014, pervenuta in cancelleria il 25 luglio 2014, nel procedimento tra Maximillian Schrems contro Data Protection Commissioner, con l'intervento di Digital Rights Ireland Ltd.

- 1) L'articolo 25, paragrafo 6, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, come modificata dal regolamento (CE) n. 1882/2003 del Parlamento europeo e del Consiglio, del 29 settembre 2003, letto alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea, **deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, come la decisione 2000/520/CE della Commissione, del 26 luglio 2000**, a norma della direttiva 95/46 sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti, con la quale la Commissione europea constata che un paese terzo garantisce un livello di protezione adeguato, **non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, come modificata, esamini la domanda di una persona relativa alla protezione dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato.**
- 2) **La decisione 2000/520 è invalida.**

Trasferimenti EU-USA

Privacy Shield

DECISIONE DI ESECUZIONE (UE) 2016/1250 DELLA COMMISSIONE del 12 luglio 2016 a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adequazione della protezione offerta dal regime dello scudo UE-USA per la privacy

Dal sito della Commissione

Lo scudo UE-USA per la privacy si fonda sui principi esposti qui di seguito.

- **Obblighi rigorosi per le imprese che operano sui dati:** nel nuovo regime il Dipartimento del Commercio degli Stati Uniti sottoporà le imprese aderenti allo scudo a verifiche e aggiornamenti periodici per accertare che rispettino nella pratica le regole che hanno volontariamente accettato. In caso contrario, l'impresa si espone a sanzioni e al depennamento dall'elenco degli aderenti. L'inasprimento delle condizioni applicabili all'ulteriore trasferimento garantirà lo stesso livello di protezione anche quando l'impresa aderente allo scudo trasferisce i dati a terzi.
- **Garanzie chiare e obblighi di trasparenza applicabili all'accesso da parte del governo degli Stati Uniti:** gli Stati Uniti hanno assicurato ufficialmente all'UE che l'accesso delle autorità pubbliche ai dati per scopi di applicazione della legge e di sicurezza nazionale è soggetto a limitazioni, garanzie e meccanismi di vigilanza precisi. La novità è che qualsiasi persona nell'UE disporrà di meccanismi di ricorso in questo settore. Gli Stati Uniti hanno escluso attività indiscriminate di sorveglianza di massa sui dati personali trasferiti negli Stati Uniti nell'ambito dello scudo. Secondo le precisazioni fornite dall'Ufficio del Direttore dell'intelligence nazionale, la raccolta di dati in blocco sarà eventualmente ammissibile solo in presenza di determinati presupposti, e comunque si tratterà obbligatoriamente di una raccolta quanto più mirata e concentrata possibile. L'Ufficio ha illustrato nei particolari le garanzie vigenti riguardo all'uso dei dati in tali circostanze eccezionali. Il Segretario di Stato degli USA ha istituito all'interno del Dipartimento di Stato una via di ricorso aperta agli europei per gli aspetti legati all'intelligence nazionale: il meccanismo di mediazione.
- **Tutela effettiva dei diritti individuali:** chiunque ritenga che, nell'ambito dello scudo, sia stato compiuto un abuso sui dati che lo riguardano ha a disposizione vari meccanismi di composizione delle controversie di agevole accesso e dal costo contenuto. Idealmente sarà l'impresa stessa a risolvere il caso di reclamo oppure saranno offerte gratuitamente soluzioni basate su un organo alternativo di composizione delle controversie (ADR). Le persone si potranno anche rivolgere alle rispettive autorità nazionali di protezione dei dati, che collaboreranno con la Commissione federale del Commercio per assicurare che i casi di reclamo sottoposti da cittadini dell'UE siano esaminati e risolti. Esperiti tutti gli altri mezzi a disposizione, come extrema ratio il caso irrisolto potrà essere sottoposto a arbitrato. Per i casi che implicano la sicurezza nazionale, i cittadini dell'UE dispongono di una possibilità di ricorso nella figura del mediatore, che è indipendente dai servizi d'intelligence degli Stati Uniti.
- **Analisi annuale comune:** il meccanismo consentirà di monitorare il funzionamento dello scudo, compresi gli impegni e le garanzie relative all'accesso ai dati a fini di contrasto della criminalità e finalità di sicurezza nazionale. La Commissione europea e il Dipartimento del Commercio degli Stati Uniti effettueranno l'analisi, alla quale assoceranno esperti dell'intelligence nazionale statunitense e le autorità europee di protezione dei dati. La Commissione attingerà a tutte le altre fonti di informazioni disponibili e presenterà una relazione pubblica al Parlamento europeo e al Consiglio.

Trasferimenti EU-USA

Privacy Shield

USA

<https://www.privacyshield.gov>



Google Analytics e l'EU-US Privacy Shield

Come descritto nella nostra certificazione Privacy Shield, [rispettiamo le disposizioni dell'EU-US Privacy Shield](#) come stabilito dal Dipartimento del Commercio degli Stati Uniti in relazione alla raccolta, all'utilizzo e alla conservazione di informazioni personali dei paesi dell'Unione Europea. Google, incluse Google Inc. e le consociate degli Stati Uniti di sua proprietà, ha certificato la sua adesione ai principi pertinenti del Privacy Shield, anche per Google Analytics.

I nostri clienti non devono intraprendere alcuna azione. Il certificato di Google è disponibile [qui](#).

Oltre al Privacy Shield, continueremo a offrire l'[Emendamento sull'elaborazione dei dati per Google Analytics](#).

Inoltre, Google Analytics e Google Analytics 360 hanno ottenuto la [Certificazione ISO 27001](#). È uno degli standard di sicurezza indipendenti più noti e accettati a livello mondiale che certifica la conformità dei sistemi di Google Analytics e Google Analytics 360.

Privacy Policy di Google

<https://www.google.com/intl/it/policies/privacy/>

FACEBOOK INC. ED EU-U.S. e SWISS-U.S. PRIVACY SHIELD (SCUDO UE-USA E SCUDO SVIZZERA-USA PER LA PRIVACY)

Facebook Inc. ("Facebook") ha la certificazione relativa al framework dell'EU-U.S. Privacy Shield Framework (scudo UE-USA per la privacy) e al framework dello Swiss-U.S. Privacy Shield Framework (scudo Svizzera-USA per la privacy) (collettivamente "Framework del Privacy Shield") con l'U.S. Department of Commerce (Dipartimento del Commercio degli Stati Uniti) in merito alla raccolta e all'elaborazione dei dati personali dei nostri inserzionisti, clienti o partner commerciali nell'Unione europea e, nei casi in cui un titolare dei dati della Svizzera si serve di Facebook come incaricato dei dati, in Svizzera ("Partner") in relazione ai prodotti e ai servizi descritti nella sezione Ambito di seguito e nella nostra [certificazione](#). Per scoprire di più sul programma Privacy Shield, visita www.privacyshield.gov.

Ambito: Facebook rispetta i Principi del Privacy Shield (come indicato in ciascuno dei relativi Privacy Shield Framework) per quanto riguarda le seguenti aree di attività (collettivamente, i "Servizi dei partner"):

- **Workplace Premium:** Workplace Premium è un servizio che consente alle persone di collaborare e condividere informazioni in modo più efficace al lavoro. I Partner (datori di lavoro oppure organizzazioni: i titolari dei dati) possono inviare informazioni personali sui propri membri a Facebook: Facebook Ireland è l'incaricato, mentre Facebook Inc. è un subincaricato. I Partner e i relativi membri decidono quali informazioni inviare, tra cui solitamente contatti aziendali, informazioni relative a clienti e dipendenti, contenuti e comunicazioni creati dai dipendenti e altre informazioni gestite dal Partner. Per maggiori informazioni, i membri possono contattare il Partner tramite cui dispongono di un account Workplace e consultare la [Normativa sulla privacy](#) di Workplace.
- **Inserzioni e misurazione:** Facebook offre prodotti per le inserzioni e la misurazione e, attraverso questi servizi, Facebook può ricevere dati personali da Partner non affiliati (i titolari dei dati), per cui Facebook Ireland è l'incaricato, mentre Facebook Inc. è un subincaricato. Comprendono elementi quali informazioni di contatto e informazioni sulle esperienze o interazioni delle persone con i Partner e i loro prodotti, servizi e inserzioni. Per maggiori informazioni sui prodotti per le inserzioni e la misurazione, visita la pagina [Informazioni sulla pubblicità su Facebook](#) e la nostra [Normativa sui dati](#).

Facebook usa i dati personali forniti dai Partner per fornire Servizi dei partner in conformità con le condizioni applicabili al Servizio dei partner pertinente e altrimenti con le istruzioni dei Partner. Facebook collabora con i suoi Partner per assicurare che le persone abbiano a disposizione scelte appropriate applicabili in base ai Principi del Privacy Shield.

Accesso: nell'ambito della nostra autorizzazione in merito e in conformità con le obbligazioni previste dal Privacy Shield, Facebook collaborerà con i suoi Partner per fornire accesso individuale ai loro dati personali in possesso di Facebook per conto dei suoi Partner. Facebook adotterà inoltre misure adeguate per consentire alle persone, direttamente o in relazione ai Partner, di correggere, modificare o eliminare dati personali che si rivelano imprecisi.

Terzi: Facebook può trasferire dati all'interno del [gruppo di aziende di Facebook](#) e a terzi, compresi fornitori di servizi e altri partner. In conformità con i Principi del Privacy Shield, Facebook è responsabile dell'eventuale elaborazione di dati personali da parte di tali terzi che risulta non coerente con i Principi del Privacy Shield, fatto salvo il caso in cui Facebook non sia da ritenersi responsabile dell'evento all'origine del danno presunto.

Facebook & Privacy Shield

<https://www.facebook.com/about/privacyshield>

Amazon

Titolari del trattamento dei dati personali

Qualsiasi dato personale fornito o raccolto tramite le operazioni che effettuerai su Amazon.it verrà trattato da Amazon Europe Core SARL, Amazon EU SARL, Amazon Services Europe SARL e Amazon Media EU SARL, quali autonomi titolari del trattamento dei dati, tutte con sede a 5, Rue Plaetis L-2338, Lussemburgo.

Scudo Unione Europea-Stati Uniti e Scudo Svizzera-Stati Uniti per la Privacy

Amazon.com, Inc. aderisce allo Scudo Unione Europea-Stati Uniti e allo Scudo Svizzera-Stati Uniti per la Privacy. Per maggiori informazioni clicca [qui](#).

Privacy Policy di Amazon

<https://www.amazon.it/gp/help/customer/display.html?nodeId=201909010>

Whatsapp



WhatsApp

WHATSAPP WEB

FUNZIONI

SCARICA

WHATSAPP INC., EU-U.S. PRIVACY SHIELD E SWISS-U.S. PRIVACY SHIELD (SCUDO UE-USA E SCUDO SVIZZERA-USA PER LA PRIVACY)

WhatsApp Inc. ("WhatsApp") ha aderito all'[EU-U.S. Privacy Shield Framework \(scudo UE-USA per la privacy\)](#) e allo [Swiss-U.S. Privacy Shield Framework \(scudo Svizzera-USA per la privacy\)](#) con l'U.S. Department of Commerce (Dipartimento del Commercio degli Stati Uniti) in merito alla raccolta e all'elaborazione dei dati personali da parte dei nostri partner commerciali nell'Unione europea e in Svizzera ("Partner") in relazione ai prodotti e ai servizi descritti di seguito nella sezione Ambito e nella nostra [certificazione](#). Per saperne di più sul programma Privacy Shield, visita www.privacyshield.gov.

Privacy Policy di Whatsapp

<https://www.whatsapp.com/legal/#privacy-policy>

Clausole tipo adottate dalla Commissione (Model Contractual Clauses)

Clausole tipo

Nomenclatura

- Clausole tipo di protezione dei dati
- Standard data protection clauses
- Model Contractual Clauses
- Model clauses

Titolare del trattamento EU-Titolare non EU o EEA

DECISIONE DELLA COMMISSIONE del 15 giugno 2001 relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere terzi a norma della direttiva 95/46/CE

DECISIONE DELLA COMMISSIONE del 27 dicembre 2004 che modifica la decisione 2001/497/CE per quanto riguarda l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi

Titolare del trattamento EU a Responsabile del t. non EU o EEA

DECISIONE DELLA COMMISSIONE del 5 febbraio 2010 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio

Apple

Utilizza le Model Contractual Clauses e aderisce a APEC CROSS-BORDER PRIVACY RULES SYSTEM

Utenti internazionali

Tutti i dati da te forniti potrebbero essere trasferiti a o consultati da entità di tutto il mondo secondo i termini descritti nella presente Politica sulla privacy. Le informazioni personali correlate ai servizi Apple relative ai residenti in uno degli Stati membri dello Spazio Economico Europeo e in Svizzera sono controllate da Apple Distribution International in Irlanda ed elaborate per suo conto da Apple Inc. Apple utilizza i documenti **"Model Contractual Clauses"** approvati per il trasferimento internazionale dei dati personali raccolti nello Spazio economico europeo e in Svizzera. Come azienda globale, Apple ha svariate entità legali in diverse giurisdizioni, le quali sono responsabili dei dati personali che raccolgono e che vengono elaborati per loro conto da Apple Inc. Ad esempio, le informazioni sul punto vendita nelle nostre entità Retail al di fuori degli Stati Uniti sono controllate dalle nostre singole entità Retail in ogni Paese. I dati personali correlati a Apple, Apple Online Store e iTunes possono essere controllati anche da entità legali al di fuori degli Stati Uniti, come illustrato nei Termini di ciascun servizio.

Apple aderisce al [sistema APEC \(Asia-Pacific Economic Cooperation\) Cross Border Privacy Rules](#). Il sistema APEC CBPR fornisce un framework per le organizzazioni in modo da garantire la protezione dei dati personali trasferiti tra le varie economie APEC partecipanti. Per saperne di più sulla Certificazione APEC e sulla risoluzione delle controversie, fai clic sul marchio TRUSTe.

Norme vincolanti di impresa (BCR)

BCR

Procedimento (art. 47, § 1)

Competenza: autorità di controllo competente (Lead Authority)

Criterio: Meccanismo di coerenza ex art. 63

Condizioni (art. 47, § 1)

- a) siano **giuridicamente vincolanti** e si applichino a tutti i membri interessati del **gruppo** imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, compresi i loro dipendenti;
- b) conferiscano espressamente **agli interessati diritti azionabili** in relazione al trattamento dei loro dati personali; **e**
- c) soddisfino i requisiti di cui al paragrafo 2

Ruolo della Commissione (art. 47, § 3)

La Commissione **può specificare il formato e le procedure** per lo scambio di informazioni tra titolari del trattamento, responsabili del trattamento e autorità di controllo in merito alle norme vincolanti d'impresa ai sensi del presente articolo. Tali atti di esecuzione sono adottati **secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.**

BCR

Contenuto delle BCR (art. 47, § 2)

- a) la **struttura e le coordinate di contatto del gruppo imprenditoriale o del gruppo di imprese** che svolgono un'attività economica comune e di ciascuno dei suoi membri;
- b) i **trasferimenti o il complesso di trasferimenti di dati**, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione;
- c) la loro **natura giuridicamente vincolante**, a livello sia interno che esterno;
- d) l'applicazione dei **principi generali di protezione dei dati**, in particolare in relazione alla **limitazione della finalità**, alla **minimizzazione dei dati**, alla **limitazione del periodo di conservazione**, alla **qualità dei dati**, alla **protezione fin dalla progettazione e alla protezione per impostazione predefinita**, alla **base giuridica del trattamento** e al **trattamento di categorie particolari di dati personali**, le **misure a garanzia della sicurezza dei dati** e i **requisiti per i trasferimenti successivi ad organismi** che non sono vincolati dalle norme vincolanti d'impresa;
- e) i **diritti dell'interessato** in relazione al trattamento e i mezzi per esercitarli, compresi il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione ai sensi dell'articolo 22, il **diritto di proporre reclamo** all'autorità di controllo competente e **di ricorrere alle autorità giurisdizionali competenti degli Stati membri** conformemente all'articolo 79, e il **diritto di ottenere riparazione** e, se del caso, il **risarcimento** per violazione delle norme vincolanti d'impresa;
- f) il fatto che **il titolare del trattamento o il responsabile del trattamento stabilito nel territorio di uno Stato membro si assume la responsabilità** per qualunque violazione delle norme vincolanti d'impresa commesse da un membro interessato non stabilito nell'Unione; il titolare del trattamento o il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità solo se dimostra che l'evento dannoso non è imputabile al membro in questione;
- g) le **modalità in base alle quali sono fornite all'interessato le informazioni** sulle norme vincolanti d'impresa, in particolare sulle disposizioni di cui alle lettere d), e) e f), in aggiunta alle informazioni di cui agli articoli 13 e 14;
- h) i **compiti di qualunque responsabile della protezione dei dati designato** ai sensi dell'articolo 35 o di ogni altra persona o entità incaricata del controllo del rispetto delle norme vincolanti d'impresa all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e il controllo della formazione e della gestione dei reclami;
- i) le **procedure di reclamo**;
- j) i **meccanismi all'interno del gruppo imprenditoriale o del gruppo di imprese** che svolgono un'attività economica comune per garantire la verifica della conformità alle norme vincolanti d'impresa. Tali meccanismi comprendono verifiche sulla protezione dei dati e metodi per assicurare provvedimenti correttivi intesi a proteggere i diritti dell'interessato. I risultati di tale verifica dovrebbero essere comunicati alla persona o entità di cui alla lettera h) e all'organo amministrativo dell'impresa controllante del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e dovrebbero essere disponibili su richiesta all'autorità di controllo competente;
- k) i **meccanismi per riferire e registrare le modifiche** delle norme e comunicarle all'autorità di controllo;
- l) il **meccanismo di cooperazione con l'autorità di controllo** per garantire la conformità da parte di ogni membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, in particolare la messa a disposizione dell'autorità di controllo dei risultati delle verifiche delle misure di cui alla lettera j);
- m) i **meccanismi per segnalare all'autorità di controllo competente ogni requisito di legge** cui è soggetto un membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune in un paese terzo che potrebbe avere effetti negativi sostanziali sulle garanzie fornite dalle norme vincolanti d'impresa; e
- n) l'**appropriata formazione** in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali.

Pareri (Opinions) dell'Art. 29 WP sulle BCR

Parere	Titolo
<u>WP 74 del 3 giugno 2003</u>	Working document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to
<u>WP 107 del 14 aprile 2005</u>	Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From
<u>WP 108 del 14 aprile 2005</u>	Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules
<u>WP 133 del 10/01/2007</u>	Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data
<u>WP 153 del 24 giugno 2008</u>	Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules
<u>WP 154 del 24 giugno 2008</u>	Working Document Setting up a framework for the structure of Binding Corporate Rules
<u>WP 155 rev. 04 del 24 giugno 2008 rev. 8 aprile 2009</u>	Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules
<u>WP 195 del 6 giugno 2012</u>	Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules
<u>WP 204 del 19 aprile 2013</u>	Explanatory Document on the Processor Binding Corporate Rules
<u>WP 244 rev. 01 del 13 dicembre 2016</u>	Guidelines for identifying a controller or processor's lead supervisory authority
<u>WP 256 rev. 01 del 6 febbraio 2018</u>	Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules
<u>WP 257 rev. 01 del 6 febbraio 2018</u>	Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules

Legenda

Contenuto delle BCR

Checklist

FAQ

Modello esemplificativo di BCR

Procedure di cooperazione a livello europeo

Standard Application for Approval of Binding Corporate Rules

PART 1: APPLICANT INFORMATION

1. STRUCTURE AND CONTACT DETAILS OF THE GROUP

Name of the Group and location of its headquarters (ultimate parent company):

Does the Group have its headquarters in the EEA?

→ ☐ → Yes
→ ☐ → No

Name and location of the applicant:

Identification number (if any):

Legal nature of the applicant (corporation, partnership, etc.):

Description of position of the applicant within the Group:
(e.g. headquarters of the Group in the EEA, or, if the Group does not have its headquarters in the EEA, the member of the Group inside the EEA with delegated data protection responsibilities)

Name and/or function of contact person (note: the contact person may change, you may indicate a function rather than the name of a specific person):

Address:

Country:

Phone number: → → → Fax: → → → → E-Mail:

EEA Member States for which approval of the BCRs is sought:

**Modello
BCR**

WP133

Deroghe in specifiche situazioni

Deroghe in specifiche situazioni

Presupposti (art. 49, § 1)

manca di decisione di adeguatezza, garanzie adeguate, BCR

Condizioni (art. 49, § 1)

- a) l'interessato, previamente informato, **acconsente** (consenso esplicito, specifico per il particolare trasferimento di dati, informato sui rischi - v. par. 2.1 Guidelines 2/2018 EDPB)
- b) trasferimento **necessario all'esecuzione di un contratto** ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato
- c) trasferimento **necessario per la conclusione o l'esecuzione di un contratto** stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato (v. par. 2.2 Guidelines 2/2018 EDPB)
- d) trasferimento **necessario per importanti motivi di interesse pubblico** (v. par. 2.4 Guidelines 2/2018 EDPB)
- e) trasferimento **necessario** per accertare, esercitare o difendere un diritto **in sede giudiziaria** (v. par. 2.5 Guidelines 2/2018 EDPB)
- f) trasferimento **necessario per tutelare gli interessi vitali** dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso (v. par. 2.6 Guidelines 2/2018 EDPB)
- g) trasferimento **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 esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri (v. par. 2.7 Guidelines 2/2018 EDPB)
- h) trasferimento verso un paese terzo o un'organizzazione internazionale sia **ammesso soltanto se non è ripetitivo, riguarda un numero limitato di interessati, è necessario** per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e **qualora il titolare e del trattamento abbia valutato tutte le circostanze** relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali. Il titolare informa l'autorità di controllo e l'interessato degli interessi legittimi perseguiti (v. par. 2.8 Guidelines 2/2018 EDPB).

Le responsabilità

Responsabilità

Articolo 82

Diritto al risarcimento e responsabilità

1. 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.
2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento **solo se non ha adempiuto gli obblighi** del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.
3. Il titolare del trattamento o il responsabile del trattamento **è esonerato dalla responsabilità**, a norma del paragrafo 2 **se dimostra che l'evento dannoso non gli è in alcun modo imputabile**.
4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, **ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno**, al fine di garantire il risarcimento effettivo dell'interessato.
5. Qualora un titolare del trattamento o un responsabile del trattamento **abbia pagato**, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento **ha il diritto di reclamare dagli altri titolari del trattamento** o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.
6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno **sono promosse dinanzi alle autorità giurisdizionali competenti** a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.

Le sanzioni

Le sanzioni del Regolamento UE 679/2016

Articolo 83 - Condizioni generali per infliggere sanzioni amministrative pecuniarie

...

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie **fino a 10.000.000 EUR**, o per le imprese, **fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore:

- a) **gli obblighi** del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;
- b) **gli obblighi** dell'organismo di certificazione a norma degli articoli 42 e 43;
- c) **gli obblighi** dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie **fino a 20.000.000 EUR**, o per le imprese, **fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore:

- a) **i principi di base del trattamento**, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;
- b) **i diritti degli interessati** a norma degli articoli da 12 a 22;
- c) **i trasferimenti di dati personali** a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;
- d) **qualsiasi obbligo** ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;
- e) **l'inosservanza di un ordine**, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

6. In conformità del paragrafo 2 del presente articolo, **l'inosservanza di un ordine da parte dell'autorità di controllo** di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie **fino a 20.000.000 EUR**, o per le imprese, **fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore.

...

Sanzioni amministrative pecuniarie



fino a 10.000.000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore



fino a 20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore

Sanzioni amministrative (art. 83, par. 4)

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

- a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;
- b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;
- c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

Sanzioni amministrative (art. 83, par. 5)

5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

- a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;
- b) i diritti degli interessati a norma degli articoli da 12 a 22;
- c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;
- d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;
- e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

Grazie per l'attenzione
Avv. Nicola Fabiano

info@fabiano.law

www.fabiano.law



@nicfab



/nicfab



/nicfab