FISCALFOCUS

Direzione Antonio Gigliotti

SCHEDE DI SINTESI

Nuovo Regolamento (UE) Privacy 679/2016

SCHEDE DI SINTESI

NUOVO REGOLAMENTO (UE) PRIVACY 679/2016

INDICE

1 SCHEDA N. 1 – AZIENDE E PROFESSIONISTI: GLI STEP PER ADEGUARSI

GLI STEP NECESSARI PER L'ADEGUAMENTO

→ **AL REGOLAMENTO UE 679/2016**

→ **PER AZIENDE E PROFESSIONISTI**

COME ADEGUARSI AL GDPR IN 9 PUNTI

1 **LA VALUTAZIONE DELLA COMPLIANCE**

Raccolta e analisi delle informazioni sull'organizzazione aziendale

2 **CREAZIONE DEL REGISTRO DEI TRATTAMENTI**

Un registro delle attività di trattamento svolte sotto la responsabilità del titolare del trattamento

3 **STESURA/MODIFICA DELLA DOCUMENTAZIONE**

Tutta la documentazione deve essere necessariamente sempre aggiornata e completa

4 **INDIVIDUAZIONE DEI RUOLI E DELLE RESPONSABILITÀ**

Individuare, sensibilizzare e formare tutte le persone "attive" del processo
Individuare anche le singole responsabilità

5 **INDIVIDUAZIONE E NOMINA DI UN DATA PROTECTION OFFICER**

Nuova figura professionale - uno degli elementi-chiave del nuovo sistema di governance dei dati - prevede una serie di condizioni in rapporto alla nomina, allo status e ai compiti specifici.

6 **DEFINIZIONE DELLE POLITICHE DI SICUREZZA E VALUTAZIONE DEI RISCHI**

Determinazione del valore quantitativo o qualitativo dei rischi connessi ad una situazione concreta o minaccia conosciuta.

7 **VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI**

Consente di valutare gli aspetti relativi alla protezione dei dati, prima che questi vengano trattati

8 **IMPLEMENTAZIONE DEI PROCESSI PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO**

Al fine di assicurarsi di aver adottato tutte le procedure idonee alla tutela dei diritti dell'interessato.

9 Analizzare e fissare gli adempimenti nel caso di un data breach (perdita, violazione ecc…di dati sensibili, protetti o riservati)

IL NUOVO REGOLAMENTO AVRÀ UN IMPATTO SU ENTI E IMPRESE

DAL PUNTO DI VISTA TECNOLOGICO

DAL PUNTO DI VISTA ORGANIZZATIVO E LEGALE

SECONDO IL NUOVO REGOLAMENTO EUROPEO OGNI AZIENDA INFATTI DOVRÀ:
→ effettuare un controllo interno;
→ verificare il proprio livello di esposizione ai rischi;
→ svolgere una serie di interventi per mitigare i rischi;
→ innalzare il livello di tutela;
→ documentare le scelte prese secondo un processo di accountability che caratterizza l'intero regolamento.

Sulla base di tutte quelle scelte prese, motivate e documentate, **le aziende saranno valutate**. Enti pubblici e imprese saranno dunque maggiormente responsabilizzati, anche attraverso, come sanzioni piuttosto elevate.

IN TUTTO CIÒ ASSUME PARTICOLARE RILEVANZA

FIGURA CENTRALE DI QUESTO NUOVO QUADRO GIURIDICO IN MOLTI AMBITI

LA FIGURA DEL DPO

MANAGER DEL CAMBIAMENTO DIGITALE

FACILITA L'OSSERVANZA DELLE DISPOSIZIONI DEL RGPD

2 SCHEDA N. 2 - ACCOUNTABILITY

ACCOUNTABILITY – NUOVO APPROCCIO FONDATO SU RESPONSABILIZZAZIONE

PRINCIPIO NUOVO REGOLAMENTO UE 679/2016 Art. 24

ossia l'approccio basato cioè sull'analisi del rischio e sulle misure da adottare in maniera preventiva da parte di responsabili e titolari

l'**adozione cioè, come la stessa norma specifica, di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.**

ACCOUNTABILITY

privacy by design

PREVENIRE NON CORREGGERE
Principio secondo cui i problemi e le soluzioni da adottare vanno valutati nella fase di progettazione

privacy by default

Necessità della tutela della vita privata dei cittadini "**di default**" appunto, cioè come **IMPOSTAZIONE PREDEFINITA**.

IL TITOLARE DEL TRATTAMENTO

deve mettere in atto

adeguate misure tecniche ed organizzative

per garantire ed essere in grado di dimostrare che le operazioni di trattamento vengano effettuate in conformità alla nuova disciplina.

ACCOUNTABILITY

si compone di almeno tre elementi:

LA "TRASPARENZA" intesa come garanzia della completa accessibilità alle informazioni, in primo luogo per i cittadini, anche in quanto utenti del servizio.

LA "RESPONSIVITÀ"
intesa come la capacità di rendere conto di scelte, comportamenti e azioni e di rispondere alle questioni poste dagli stakeholder.

LA "COMPLIANCE" intesa come capacità di far rispettare le norme, sia nel senso di finalizzare l'azione pubblica all'obiettivo stabilito nelle leggi, che nel senso di fare

3 SCHEDA N. 3 – DATA PROTECTION BY DEFAULT AND BY DESIGN

DATA PROTECTION BY DEFAULT AND BY DESIGN

Regolamento Ue 679/2016 – Art. 25

l'adozione di misure tecniche ed organizzative adeguate al fine di tutelare i dati da trattamenti illeciti fin dall'inizio del trattamento

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

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.

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.

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.

PRIVACY BY DESIGN

PREVENIRE NON CORREGGERE

Principio secondo cui i problemi e le soluzioni da adottare vanno valutati nella fase di progettazione

È BASATO SULLA VALUTAZIONE DEL RISCHIO

PRIVACY BY DEFAULT

Necessità della tutela della vita privata dei cittadini "di default" appunto, cioè come **IMPOSTAZIONE PREDEFINITA.**

le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste

RISK BASED

Valutazione prima che il trattamento inizi

valutazione andrà fatta al momento della progettazione del sistema

le aziende dovranno valutare il rischio inerente alle loro attività.

↓

si dovrà tenere conto

↓

DELLO STATO DELLA TECNOLOGIA, PER CUI IL TRATTAMENTO VA ADATTATO NEL CORSO DEL TEMPO.

4 SCHEDA N. 4 – LEICITÀ DEL TRATTAMENTO

LEICITÀ DEL TRATTAMENTO

Art. 6 - CAPO II del Regolamento

il trattamento dei dati personali è lecito solo se risponde a determinate caratteristiche.

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

In linea di massima i fondamenti di leicità indicati nell'art. 6 coincidono con quelli del previsti dal vecchio Codice della privacy (D. Lgs. 196/2003), quali consenso, interessi del titolare, obblighi contrattuali ecc.

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

Art. 6 Regolamento

- l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

L'ultimo punto non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

5 SCHEDA N. 5 – IL CONSENSO AL TRATTAMENTO DEI DATI

IL CONSENSO AL TRATTAMENTO DEI DATI

REGOLAMENTO UE 679/2016 – Art. 7

L'Informativa e il consenso sono fra i primi adempimenti chiave di tutto il processo, essendo questi fra più importanti presupposti perché il trattamento dei dati possa essere considerato legittimo.

CARATERISTICHE CONSENSO

SPECIFICO CIOÈ INTELLEGIBILE
• relativo alla specifica finalità per cui si richiede, quando ha più finalità difatti andrà richiesto e prestato per ogni finalità; i dati dovranno inoltre essere pertinenti al consenso fornito;
INFORMATO
• cioè l'interessato dovrà ricevere tutte le informazioni necessarie dal titolare in riguardo alla finalità per cui è effettuato e in cosa consiste il trattamento;
INEQUIVOCABILE
• l'interessato dovrà esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, non dovrà sussistere alcun dubbio circa le modalità di raccolta, quali caselle prespuntate ecc. ;
ESPLICITO - (ART. 9 GDPR)
• nel caso di trattamento di dati sensibili o nel caso di **processi decisionali automatizzati** (es. profilazione);
LIBERO
• il consenso dovrà essere prestato cioè liberamente senza atti intimidatori o raggiri deve manifestare una scelta effettiva e non deve portare a conseguenze negative nei casi in cui ci sia un mancato conferimento, richiamando l'articolo 7 del Regolamento Ue a tal riguardo chiarisce che: *"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"*;
VERIFICABILE
• su questo punto è bene specificare che ciò non significa che debba essere documentato per iscritto né che è richiesta la forma scritta bensì che l'azienda debba essere in grado di dimostrare che l'interessato lo ha conferito in merito a quel specifico trattamento (anche se si consiglia l'utilizzo scritto, come prova del consenso anche durante una verifica da parte dell'autorità).

REVOCABILE

- **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. Ciò si collega ad un'importante novità introdotta dal GDPR quale il diritto all'oblio, il diritto cioè alla cancellazione. È da specificare inoltre che non vi è alcun obbligo che pesa sull'interessato in riguardo alla motivazione da fornire in caso di revoca. In caso di revoca il titolare dovrà cancellare i dati dell'utente senza giustificato ritardo entro le 72h da cui ne è venuto a conoscenza.

Le aziende e i professionisti dovranno raccogliere di nuovo il consenso?

NO

se è stato espresso secondo modalità conformi alle condizioni del presente regolamento, affinché il titolare del trattamento possa proseguire il trattamento in questione dopo la data di applicazione del presente regolamento

6 SCHEDA N. 6 – CONSENSO DEI MINORI

CONSENSO DEI MINORI

Regolamento Ue 679/2016 – Art. 8

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

"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".

OBBLIGHI DEL TITOLARE PER LA VERIFICA DELL'ETÀ

Il titolare del trattamento deve adoperarsi in ogni modo ragionevole per verificare che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore in maniera corretta

in considerazione delle tecnologie disponibili.

IL LEGISLATORE ITALIANO HA FISSATO IL LIMITE DI ETÀ

DA APPLICARE IN ITALIA → **A 14 ANNI**

DIRITTO ALLA CANCELLAZIONE DEI DATI

quando l'interessato ha prestato il proprio consenso quando era ancora minorenne, dunque non pienamente consapevole dei rischi derivanti dal trattamento,

IMPORTANTE la cancellazione dei dati come specificato nel considerando 65

Tale diritto è specificato, per ogni interessato dei dati al di là che sia minore o meno, nell'art. 17 del Regolamento nel cosiddetto **DIRITTO ALL'OBLIO**

INFORMATIVA E CONSENSO DEL GENITORE

in alcuni casi dovrà riportare il consenso dei genitori, la raccolta non dovrà essere eccessivamente burocratica e al contempo dovrà essere predisposta e ricevuta dal genitore stesso con modalità tali da evitare eventuali manipolazioni o falsificazioni ad opera del minore stesso

7 SCHEDA N. 7 – DIRITTI DEGLI INTERESSATI

DIRITTI DEGLI INTERESSATI

Regolamento Ue 679/2016 – Artt. da 12 a 23

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

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

ELENCO DIRITTI INTERESSATI

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

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

8 SCHEDA N. 8 – DIRITTO ALLA CANCELLAZIONE ("DIRITTO ALL'OBLIO")

DIRITTO ALL'OBLIO

→ Regolamento UE 2016/679 – **Art. 17**

→ l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo in casi specificamente individuati.

→ Il titolare del trattamento nei casi indicati è obbligato a procedere alla cancellazione dei dati e ad adottare le misure ragionevoli per informare altri titolari del trattamento che stanno trattando i dati in questione di procedere alla cancellazione.

L'INTERESSATO HA IL DIRITTO DI OTTENERE LA CANCELLAZIONE SE SUSSISTE UNO DEI SEGUENTI MOTIVI:
↘ i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
↘ l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento;
↘ l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
↘ i dati personali sono stati trattati illecitamente;
↘ 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;
↘ i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.

QUANDO NON SI APPLICA IL DIRITTO ALL'OBLIO

1. qualora il trattamento sia necessario per l'esercizio della libertà di espressione e di informazione
2. per l'adempimento di un obbligo legale
3. per l'esecuzione di un compito svolto nel pubblico interesse
4. interessi storici, statistici e di ricerca scientifica
5. per l'esercizio o la difesa di un diritto in sede giudiziaria.

Nota bene

In tali casistiche i titolari del trattamento possono consentire al mantenimento dei dati personali nonostante l'opposizione dell'interessato.

9 SCHEDA N. 9 – DIRITTO DI OPPOSIZIONE

DIRITTO DI OPPOSIZIONE AL TRATTAMENTO DEI DATI

Regolamento UE 679/2016 – Art. 21

in alcune specifiche tipologie di trattamento di dati personali, l'interessato del trattamento possa esercitare il diritto di opporsi, **solo adducendo motivi legittimi connessi alla sua situazione particolare**

ovvero quando il trattamento è necessario per l'esecuzione di un compito di interesse pubblico, effettuato per scopi di ricerca scientifica, storica o statistica oppure connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento o anche se il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, anche quando nell'ambito di tale trattamento è prevista la profilazione.

Marketing

Qualora, invece, si tratti di trattamento finalizzato ad **attività di marketing diretto - compresa la profilazione.**

l'interessato **può opporsi in qualsiasi momento**

in tal caso, dunque, il suo diritto è assoluto

IL TITOLARE È TENUTO AD INFORMARE L'INTERESSATO

in maniera chiara, specifica (l'informazione deve essere evidentemente separata dalle altre) e trasparente della possibilità di esercitare il diritto di opporsi al trattamento

delle modalità attraverso le quali poterlo fare

dell'eventuale esistenza di un suo interesse legittimo al trattamento.

SOLUZIONI PER ESSERE CONFORMI AL REGOLAMENTO

Rivedere le informative, controllando che agli interessati sia stato comunicato tale diritto correttamente, in maniera separata come richiesto dalle disposizioni del Regolamento e informare l'interessato dell'eventuale esistenza dell'interesse legittimo del titolare;

Accertarsi dell'esistenza di un meccanismo che consenta all'interessato di esercitare agevolmente l'opt-out in particolare quando si tratta di operazioni svolte attraverso comunicazioni elettroniche (es. nelle newsletter o negli SMS), prevedendo sistemi automatizzati rispettosi delle disposizioni di cui alla direttiva n. 2002/58/CE;

Tenere traccia delle opposizioni esercitate

10 SCHEDA N. 10 – DIRITTO ALLA PORTABILITÀ DEI DATI

DIRITTO ALLA PORTABILITÀ DEI DATI

→ Regolamento (Ue) 2016/679 **– Art. 20**

→ Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

→ sono portabili **solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato**

→ sono portabili **solo i dati che siano stati "forniti" dall'interessato al titolare**

→ **Non si applica ai trattamenti non automatizzati**

DIRITTO ALLA PORTABILITÀ DEI DATI

NON SI APPLICA AI TRATTAMENTI NON AUTOMATIZZATI

archivi | **registri cartacei**

sono portabili solo i dati trattati con il consenso dell'interessato o sulla base **di un contratto stipulato con l'interessato**

e solo i dati che siano stati "forniti" dall'interessato al titolare

il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

si chiarisce che il nuovo diritto alla portabilità intende promuovere il controllo degli interessati sui propri dati personali, facilitando la circolazione, la copia o la trasmissione dei dati da un ambiente informatico all'altro (che si tratti dei propri sistemi, dei sistemi di soggetti terzi fidati, o di quelli di un diverso titolare del trattamento).

11

SCHEDA N. 11 – DIRITTO DI RETTIFICA

DIRITTO DI RETTIFICA

Regolamento (Ue) 2016/679 – **Art. 16**

diritto di ottenere dal titolare del trattamento la rettifica dei dati personali, e senza ingiustificato ritardo, tenuto conto delle finalità del trattamento

diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

DIRITTO DELL'INTERESSATO

di richiedere al titolare **CHE I DATI CHE LO RIGUARDANO**

siano modificati

Corretti o aggiornati

nonché che siano integrati i **dati personali incompleti**.

TUTELA IDENTITÀ PERSONALE DEGLI INDIVIDUI

diritto a che le dichiarazioni ad essi riferite siano veritiere

non siano inesatte

non siano idonee ad alterare l'identità personale

DATI RISPONDENTI AL VERO

12

SCHEDA N. 12 – DIRITTO DI ACCESSO

DIRITTO DI ACCESSO

Regolamento Ue 679/2016 – Art. 15

diritto del soggetto interessato di richiedere e ottenere dal titolare del trattamento informazioni sul trattamento di dati personali che viene effettuato.

DIRITTO RAFFORZATO DAL REGOLAMENTO

DIRITTO DI ACCESSO

DIRITTO di prendere visione, o estrarre copia, di vari tipi di documenti.

IN AMBITO AMMINISTRATIVO - assicura la **trasparenza** e l'imparzialità delle pubbliche amministrazioni, funzionali alla cura degli interessi pubblici.

DIRITTO di richiedere e ottenere dal titolare del trattamento (il soggetto che gestisce i suoi dati) informazioni sul trattamento di dati personali che viene effettuato.

il titolare del trattamento deve fornire all'interessato una copia dei dati personali oggetto di trattamento che lo riguardano.

INFORMAZIONI DA FORNIRE ALL'INTERESATO

- le finalità del trattamento;
- le categorie di dati personali trattati;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- il periodo di conservazione dei dati personali previsto, ove possibile, oppure i criteri utilizzati per determinare tale periodo;
- l'esistenza e la possibilità per l'interessato di esercitare il diritto di rettifica, il diritto alla cancellazione, il diritto alla limitazione del trattamento, il diritto di opposizione al trattamento;
- il diritto di proporre reclamo innanzi alle autorità di controllo;
- le informazioni sull'origine dei dati, ove non siano stati raccolti presso l'interessato;
- l'eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione e le informazioni significative sulla logica utilizzata.

13

SCHEDA N. 13 – LIMITAZIONI AL TRATTAMENTO

LIMITAZIONI AL TRATTAMENTO

→ **Regolamento Ue 679/2016 – Art. 18**

→ **diritto di limitazione del trattamento quando ricorre una delle seguenti ipotesi**

LIMITAZIONE DEL TRATTAMENTO
▪ l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza degli stessi;
▪ il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
▪ benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
▪ l'interessato si è opposto a un trattamento (necessario per l'esecuzione di un compito di interesse pubblico o basato sul legittimo interesse del titolare, compresa la profilazione), in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

La limitazione del trattamento → potrebbe concretamente essere attuata

ad esempio attraverso il trasferimento temporaneo dei dati verso un altro sistema di trattamento, nel rendere i dati selezionati inaccessibili o nel rimuoverli temporaneamente.

Nota bene

Le misure da adottare sono descritte nel considerando 67, nello stesso viene inoltre evidenziato che, negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe, in linea di massima, essere assicurata mediante **dispositivi tecnici** in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. *Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato.*

La limitazione può essere, successivamente, revocata e, in tal caso, prima che la **revoca** abbia efficacia, il titolare del trattamento deve informarne il soggetto interessato.

14 SCHEDA N. 14 – LA FIGURA DEL DPO

LA FIGURA DEL DPO: RUOLO COMPITI E COMPETENZE

Regolamento Ue 679/2016 – Artt. 37-38-39

figura di garanzia professionale introdotta dal Regolamento (all'art. 37) designata in funzione delle qualità professionali con conoscenza specifica della normativa e in materia di protezione dei dati il DPO, è il fulcro del processo di "responsabilizzazione" o (accountability).

ART. 37 REGOLAMENTO (UE) 2016/679

DESIGNAZIONE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI

il titolare e il responsabile sono tenuti ad individuare o a formare un DPO qualora:

1. il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico (eccetto le autorità giurisdizionali quando esercitano le loro funzioni);
2. 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;
3. 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.

Al di fuori di tali ipotesi, invece, la designazione del DPO rimane facoltativa.

CHI PUÒ RICOPRIRE TALE RUOLO

DIPENDENTE INTERNO	SOGGETTO ESTERNO
adeguatamente formato	**Esperto altamente qualificato**
NO conflitti di interessi	**Con subdelega delle relative responsabilità entro limiti precisi**

conoscenza specialistica della normativa e della prassi
indubbie qualità professionali
capacità di assolvere adeguatamente i compiti espressi nell'elenco dell'art. 39
competenze informatiche
competenze di risk management
competenze di analisi dei processi.

I REQUISITI DEL D.P.O.

ART. 37 PARAGR.5

"è designato in funzione delle qualità professionali in particolare della conoscenza specialistica della normativa e della prassi in materia di protezione dei dati e della capacità di assolvere i compiti di cui all'articol

Non sono richieste attestazioni formali o iscrizione in appositi albi professionali pur essendo auspicato un percorso formativo specifico così da garantirne un adeguato livello di conoscenza.

DPO

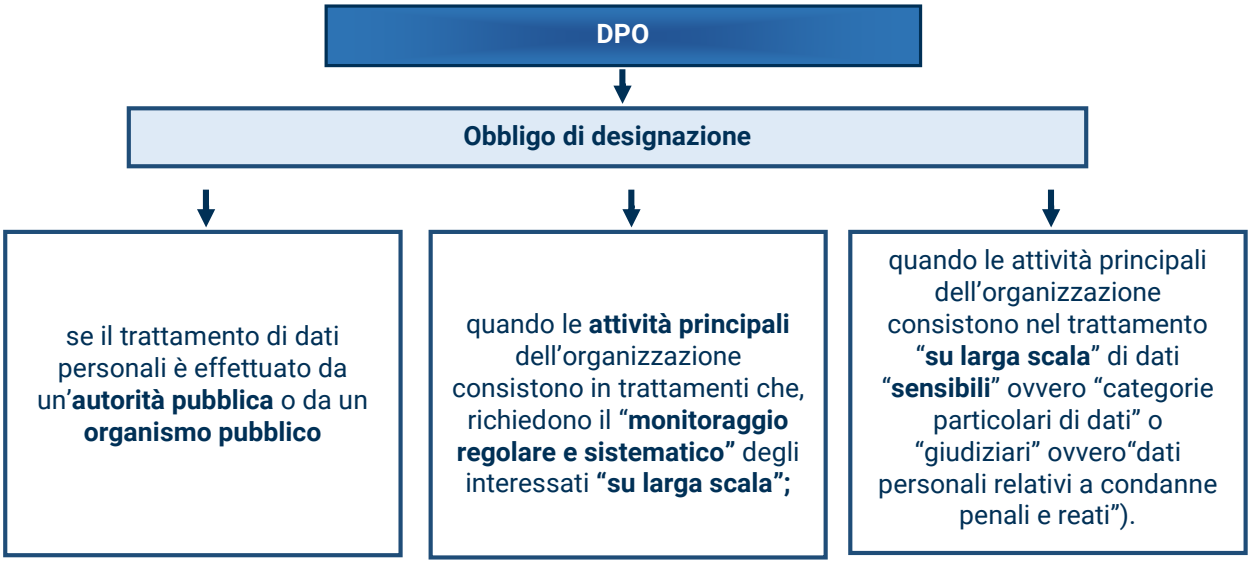
SECONDO LE NUOVE NORME GODE DI:

POSIZIONE	INDIPENDENZA	AUTONOMIA
riferisce direttamente al vertice.	non riceve istruzioni per quanto riguarda l'esecuzione dei compiti.	attribuzione di risorse umane e finanziarie adeguate.

SECONDO L'ARTICOLO 39

IL DPO DOVRÀ PRINCIPALMENTE:

- **INFORMARE E CONSIGLIARE** il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- **VERIFICARE** l'attuazione e l'applicazione del Regolamento;
- **ATTRIBUIRE DELLE RESPONSABILITÀ, SENSIBILIZZARE** E **FORMARE** il personale coinvolto nelle operazioni di trattamento;
- **GESTIRE GLI AUDIT INTERNI E FORNIRE PARERI** in merito alla valutazione d'impatto sulla protezione dei dati;
- **SORVEGLIARE GLI ADEMPIMENTI** relativi all'applicazione delle norme;
- **FUNGERE DA PUNTO DI CONTATTO PER GLI INTERESSATI** in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;
- **FUNGERE DA PUNTO DI CONTATTO PER IL GARANTE** PER LA PROTEZIONE DEI DATI PERSONALI OPPURE, EVENTUALMENTE, CONSULTARE L'AUTORITÀ DI PROPRIA INIZIATIVA.


DPO
Obbligo di designazione
se il trattamento di dati personali è effettuato da un'**autorità pubblica** o da un **organismo pubblico**
quando le **attività principali** dell'organizzazione consistono in trattamenti che, richiedono il "**monitoraggio regolare e sistematico"** degli interessati **"su larga scala";**
quando le attività principali dell'organizzazione consistono nel trattamento "**su larga scala**" di dati "**sensibili**" ovvero "categorie particolari di dati" o "giudiziari" ovvero"dati personali relativi a condanne penali e reati").

15 SCHEDA N. 15 – OBBLIGHI DEL TITOLARE DEL TRATTAMENTO

OBBLIGHI DEL TITOLARE DEL TRATTAMENTO

Regolamento (Ue) 2016/679 –

Il Titolare del trattamento (*data controller*) è colui che

da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali"

TITOLARE DEL TRATTAMENTO

È chi decide il motivo e le modalità del trattamento, ed è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa, sia nazionale che internazionale, in materia di protezione dei dati personali, compreso l'obbligo di notifica al Garante nei casi previsti.

OBBLIGHI DEL TITOLARE

obbligo di notifica al Garante nei casi previsti

deve porre in essere misure tecniche e organizzative adeguate per garantire, sin dalla fase della progettazione, la tutela dei diritti dell'interessato (privacy by design).

di riservatezza dei dati

inteso come dovere di non usare, comunicare o diffondere i dati al di fuori del trattamento.

deve garantire che i dati non siano persi, alterati, distrutti o comunque trattati illecitamente.

SPETTA A LUI STABILIRE LE MISURE ADEGUATE DI SICUREZZA.

IL TITOLARE

nomina con contratto o atto giuridicamente valido, il responsabile del trattamento

pone in atto le misure tecniche ed organizzative congrue per garantire un livello di sicurezza adeguato al rischio.

È tenuto insieme al RPD

alla redazione del registro di trattamenti.

16

SCHEDA N. 16 – INFORMATIVA

I CONTENUTI DELL'INFORMATIVA SONO ELENCATI

→ Regolamento UE 679/2016 - **Articoli 13, paragrafo 1, e 14, paragrafo 1**

IL TITOLARE DEVE SEMPRE SPECIFICARE

1. i dati di contatto del RPD-DPO
2. ove esistente, la base giuridica del trattamento
3. **qual è il suo interesse legittimo**
4. **se trasferisce i dati personali in Paesi terzi**

IL TITOLARE DEVE INOLTRE SPECIFICARE

- il periodo di conservazione dei dati
- i criteri seguiti per stabilire tale periodo di conservazione, e il **diritto di presentare un reclamo** all'autorità di controllo.

TRATTAMENTO → **PROCESSI DECISIONALI AUTOMATIZZATI** → **L'INFORMATIVA DEVE SPECIFICARLO**

TEMPI DELL'INFORMATIVA

QUANDO I DATI — **ART. 14 REGOLAMENTO**

↘ **NON VENGONO RACCOLTI DIRETTAMENTTE PRESSO L'INTERESSATO**

↓ **ENTRO UN MESE DALLA RACCOLTA**

↓ DEVE ESSERE FORNITA L'INFORMATIVA ALL'INTERESSATO

L'INFORMATIVA

È DATA, **IN LINEA DI PRINCIPIO**

- **PER ISCRITTO**
- E **PREFERIBILMENTE IN FORMATO ELETTRONICO**

L'INFORMATIVA

(Disciplinata nello specifico dagli artt. 13 e 14 del regolamento) deve essere fornita all'interessato prima di effettuare la raccolta dei dati (**se raccolti direttamente presso l'interessato** – art. 13 del regolamento).

Se i dati **non sono raccolti direttamente** presso l'interessato (art. 14 del regolamento), l'informativa deve comprendere anche le **categorie** dei dati personali oggetto di trattamento.

IN TUTTI I CASI

il titolare deve specificare

- la propria identità e quella dell'eventuale rappresentante nel territorio italiano
- le **finalità del trattamento**
- i **diritti degli interessati** (compreso il diritto alla portabilità dei dati)

se esiste un **responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati**.

INFORMAZIONI FONDAMENTALI INFORMATIVA

1. **Gli scopi e le modalità** del trattamento;
2. Se l'interessato **è obbligato o no** a fornire i dati;
3. Quali sono **le conseguenze** se i dati non vengono forniti;
4. A chi possono essere **comunicati o diffusi** i dati;
5. Quali sono **i diritti riconosciuti** all'interessato;
6. Chi sono **il titolare** e l'eventuale responsabile del trattamento;

UNICI CASI IN CI PUÒ ESSERE OMESSA L'INFORMATIVA

1. **Se si dispone già delle informazioni o sono informazioni note;**
2. Se comunicare tali informazioni comporta uno sforzo sproporzionato o è impossibile (valutazione che spetta al titolare del trattamento);
4. Se l'ottenimento dei dati o, la loro comunicazione, sono previsti dal diritto dell'Unione;
6. Se i dati devono restare riservati per un obbligo di segreto professionale.

17 SCHEDA N. 17 – SPECIFICHE SITUAZIONI DI TRATTAMENTO

SPECIFICHE SITUAZIONI DI TRATTAMENTO

REGOLAMENTO UE 679/2016 – Art. 85

Trattamento e libertà d'espressione e di informazione

Il diritto degli Stati membri concilia la protezione dei dati personali ai sensi del presente regolamento con il diritto alla **libertà d'espressione e di informazione**, incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria.

Ai fini del trattamento effettuato a scopi giornalistici o di espressione accademica, artistica o letteraria

gli Stati membri prevedono esenzioni o deroghe rispetto

ai capi II (principi), III (diritti dell'interessato), IV (titolare del trattamento e responsabile del trattamento), V (trasferimento di dati personali verso paesi terzi o organizzazioni internazionali), VI (autorità di controllo indipendenti), VII (cooperazione e coerenza) e IX (specifiche situazioni di trattamento dei dati)

qualora siano necessarie per conciliare il diritto alla protezione dei dati personali e la libertà d'espressione e di informazione.

DISPOSIZIONI RELATIVE A SPECIFICHE SITUAZIONI DI TRATTAMENTO

Articolo 85 - Trattamento e libertà d'espressione e di informazione
Articolo 86 - Trattamento e accesso del pubblico ai documenti ufficiali
Articolo 87 -Trattamento del numero di identificazione nazionale
Articolo 88 - Trattamento dei dati nell'ambito dei rapporti di lavoro
Articolo 89 - Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici
Articolo 90 - Obblighi di segretezza
Articolo 91 - Norme di protezione dei dati vigenti presso chiese e associazioni religiose

18

SCHEDA N. 18 – REGISTRO TRATTAMENTO DATI

REGISTO DELLE ATTIVITÀ DI TRATTAMENTO

→ **Regolamento Ue 679/2016 – Art. 30**

→ Uno strumento di fondamentale importanza, non solo per avere un quadro completo e aggiornato dei trattamenti all'interno di un'azienda o di un soggetto pubblico, ma anche per poter dimostrare e documentare dinanzi all'Autorità di controllo la conformità dell'organizzazione alle norme del Regolamento Europeo

→ In base all'art. 30 par. 4, per quanto suddetto, infatti: "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".

TENUTA REGISTRO

→ **PRINCIPIO ACCOUNTABILITY** → adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento

CHI È OBBLIGATO ALLA TENUTA DEL REGISTRO DEI TRATTAMENTI

→ **ORGANISMI CON PIÙ DI 250 DIPENDENTI**

→ che possano presentare *"un rischio per i diritti e le libertà dell'interessato, o 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"*

SOSTANZIALMENTE SECONDO LA NORMA AB ORIGINE ENTI E ALTRI ORGANISMI CON MENO DI 250 DIPENDENTI SONO ESENTATI PURCHÉ:
1. il titolare non effettui trattamenti che possano presentare un rischio per i diritti e le libertà degli interessati;
2. il trattamento non sia occasionale o includa dati di cui all'art. 9.1 o all'articolo 10 (dati particolari e dati personali giudiziari).

NELLO SPECIFICO, ALL'INTERNO DEL REGISTRO SI POTREBBERO INSERIRE I SEGUENTI ELEMENTI:
→ **processi/macro-attività**, per poter inquadrare i trattamenti di dati personali all'interno delle attività svolte da ciascuna Unità Organizzativa e facilitarne la comprensione e l'aggiornamento da parte del relativo responsabile;
→ **base giuridica e modalità di raccolta del consenso**, per facilitare la predisposizione dell'informativa da consegnare all'interessato. La base giuridica del trattamento è tra gli elementi che devono essere contenuti all'interno dell'informativa secondo l'art. 13 co. 2.;
→ **referente interno e categorie di soggetti autorizzati al trattamento**, per fornire indicazioni utili in merito a persone che, limitatamente ai trattamenti di propria competenza, avranno dei compiti esecutivi all'interno del modello di funzionamento;

→ **responsabili esterni del trattamento**, per individuare tutti i soggetti terzi che trattano dati personali per conto del titolare del trattamento e che dovranno essere nominati responsabili esterni, richiamando le tipologie di trattamento consentite;
→ **modalità di trattamento dei dati**, per poter mappare con esattezza, attraverso l'elencazione dei soli applicativi utilizzati per il trattamento dei dati personali, le misure di sicurezza implementate/da implementare, nonché per poter condurre efficacemente la valutazione dei rischi.

AD ESEMPIO:
• **Trattamento**: il nome del trattamento (es. gestione paghe);
• **Ufficio:** l'ufficio (o gli uffici) coinvolto da quel trattamento (es. Ufficio Personale);
• **Finalità:** le finalità per le quali sono trattati tali dati (es. anagrafiche, iscrizioni sindacali, certificati di malattia, maternità ecc.);
• **Tipi di dati personali**: quali tipologie di dati personali sono coinvolti nel trattamento (es. dipendenti, liberi professionisti, collaboratori, tirocinanti, ecc.);
• **Categorie d'interessati**;
• **Consenso;**
• **Informativa;**
• **Conservazione;**
• **Misure di sicurezza e organizzative**;
• **Titolare e Responsabile del trattamento, ove previsto i dati del DPO**;
• **Ecc.**

Nota bene **È da precisare che** la predisposizione del Registro non debba essere considerata alla stregua di un nuovo adempimento burocratico, ma come uno strumento interno che consente una gestione più efficace per l'*Action plan*, per mappare i flussi di dati all'interno dell'organizzazione, per censire in maniera ordinata le banche dati, per dimostrare di aver adempiuto alle prescrizioni del Regolamento, ecc., sempre nell'ottica del principio di *accountability;* in conclusione, consentirebbe quindi di avere un **supporto importante per il governo di tutta la "data protection"**.

19

SCHEDA N. 19 – LA PROFILAZIONE

PROFILAZIONE DATI – TRATTAMENTO AUTOMATIZZATO

Regolamento UE 679/2016 – Art. 4

"qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica "

INFORMATIVA

Deve essere esplicitamente dichiarata nella Informativa agli Interessati

ACCESSO

Sapere se un processo automatizzato/profilazione sia o meno in corso e ricevere info significative su logica utilizzata, l'importanza e conseguenze previste per l'interessato

OPPOSIZIONE

In caso di **finalità di INTERESSE PUBBLICO o liceità di trattamento basata su LEGITTIMO INTERESSE:** Diritto di opporsi **in qualsiasi momento**, per motivi connessi alla sua situazione particolare, al trattamento dei dati inclusa la profilazione Il Titolare non tratta ulteriormente i dati **a meno che non dimostri l'esistenza di motivi** legittimi cogenti che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
Marketing diretto: l'interessato ha il diritto di opporsi **in qualsiasi momento** al trattamento inclusa la profilazione.

Questi diritti sono esplicitamente evidenziati all'interessato in modo separato da qualsiasi altra informazione, al momento della prima comunicazione con l'interessato.

DPIA

Se un trattamento, che prevede 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.

20 SCHEDA N. 20 – SANZIONI

SANZIONI

Regolamento UE 679/2016 **– Artt. dal 77 all'84**

Le sanzioni penali rimangono di competenza di ogni singolo Stato, mentre le nuove sanzioni amministrative, i mezzi di ricorso e le responsabilità che ne derivano sono disciplinate dal nuovo Regolamento, in particolare dal CAPO VIII (Mezzi di ricorso, responsabilità e sanzioni) dall'articolo 77 all'articolo 84.

VENGONO INASPRITE LE SANZIONI AMMINISTRATIVE PECUNIARIE

SANZIONI GDPR

REGOLAMENTO UE 2016/679

nei casi più gravi a **sanzioni fino a 20 mln di euro o al 4% del fatturato** di un'impresa

DIRITTO AL RISARCIMENTO DELL'INTERESSATO

SANZIONI PENALI

competenza di ogni singolo Stato

SANZIONI AMMINISTRATIVE

disciplinate dal nuovo Regolamento

e inflitte dall'Autorità garanti.

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

DEVE PROVVEDERE, IN OGNI SINGOLO CASO

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

ART. 83 REGOLAMENTO

VALUTAZIONE SANZIONE AMMINISTRATIVA IN BASE

- alla **natura, la gravità e la durata della violazione** tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
- il carattere **doloso o colposo** della violazione;
- alle **misure intraprese dal Titolare o dal Responsabile** per mitigare i danni subiti dagli interessati;
- il **grado di responsabilità** del Titolare o del Responsabile, anche sotto il profilo tecnico, e le misure organizzative attuate per prevenire le violazioni;
- **eventuali violazioni precedenti** commesse da parte del Titolare o del Responsabile;
- **al grado di cooperazione con l'autorità di vigilanza**, al fine di porre rimedio alla violazione e mitigarne i possibili effetti negativi;
- alle **categorie di dati personali** oggetto della violazione;
- alla **maniera in cui l'autorità di controllo ha preso conoscenza della violazione**, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
- l'**adesione a codici di condotta** o a meccanismi di certificazione riconosciuti;
- ogni **altro fattore aggravante o attenuante** applicabile alle circostanze del caso (es. eventuali benefici finanziari conseguiti o le predite evitate ecc..).

SANZIONI REGOLAMENTO

sanzioni amministrative FINO A 10 MILIONI DI EURO

FINO AL 2% DEL FATTURATO TOTALE ANNUO MONDIALE dell'esercizio precedente → **in caso di un'impresa**

Per le violazioni delle disposizioni relative agli obblighi del Titolare o del Responsabile di cui agli articoli **8, 11, da 25 a 39, 42.**

Art. 8	**Consenso dei minori**
Art. 11	**Trattamento** che non riguarda l'identificazione
Art. 25	**Protezione dei dati fin dalla progettazione** e protezione per impostazione predefinita
Art. 26	**Contitolari del trattamento**
Art. 27	Istruzioni e autorità del Titolare
Art. 28	Responsabili del trattamento
Art. 29	**Trattamento sotto l'autorità del titolare 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.
Art. 30	**Registri delle attività di trattamento.**
Art. 31	**Cooperazione con l'autorità di controllo -** notificazione dei data breach all'autorità.
Art. 32	**Sicurezza del trattamento.**
	Notifica di una violazione dei dati personali all'autorità di controllo.
Art. 34	**Comunicazione di una violazione** dei dati personali all'interessato.
Art. 35	**Valutazione d'impatto sulla protezione dei dati.**
Art. 36	**Consultazione preventiva.**
Art. 37	**Designazione, posizione e compiti del DPO –** Data Protection Officer o Responsabile Protezione Dati (RPD).
Art. 39	**Compiti del responsabile della protezione dei dati Protection Officer.**
Art. 42	**Certificazione.**

SANZIONI REGOLAMENTO

sanzioni amministrative **FINO A 20 MILIONI DI EURO**

FINO AL 4% DEL FATTURATO TOTALE ANNUO MONDIALE dell'esercizio precedente, se superiore → **per le violazioni in materia di:**

1	principi base del trattamento, comprese le condizioni relative al consenso;	**Artt. 5, 6, 7 e 9;**
2	diritti degli interessati;	**Artt. da 12 a 22**
2	trasferimento di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale;	**Artt. da 44 a 49**
3	qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX.	

DIRITTO AL RISARCIMENTO DELL'INTERESSATO

Codice Privacy – Art. 15

"*Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del Codice civile*", si osserva, innanzitutto, che **la prospettiva del Regolamento è focalizzata sul "danneggiato"** (**e non su chi ha cagionato il danno**).

Il Codice Privacy individua il responsabile del danno in "***chiunque***".

Nuovo Regolamento Ue privacy – Art. 82

"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." Oltre il diritto dell'interessato (danneggiato) di ottenere il risarcimento del danno, **ci si focalizza su chi ha cagionato il danno.**

Sono tenuti al risarcimento del danno **il titolare o il responsabile del trattamento**.

DIFFERENZE

Osserva

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

21 SCHEDA N. 21 – TRASFERIMENTO DATI VERSO PAESI TERZI

TRASFERIMENTO DEI DATI VERSO PAESI TERZI E ORGANISMI INTERNAZIONALI

Regolamento UE 679/2016 – **Art. 44**

Per garantire un livello di protezione adeguato, richiesto a seguito della globalizzazione, alla diffusione delle piattaforme on-line, la cooperazione internazionale ecc., il Legislatore europeo impone una serie di condizioni affinché un trasferimento dati verso paesi terzi possa essere effettuato.

NOVITÀ

Viene meno il requisito dell'autorizzazione nazionale (artt. 45 e 46 del Regolamento)

il trasferimento verso un **Paese terzo "adeguato"** potrà avere inizio senza attendere l'autorizzazione nazionale del Garante

ai sensi della decisione assunta in futuro dalla Commissione, ovvero sulla base di clausole contrattuali modello, debitamente adottate, o di norme vincolanti d'impresa approvate attraverso la specifica procedura di cui all'art. 47 del Regolamento

a differenza di quanto attualmente previsto dall'art. 44 del Codice.

L'AUTORIZZAZIONE SARÀ ANCORA NECESSARIA SE

- Un titolare desidera utilizzare **clausole contrattuali ad-hoc** (cioè non riconosciute come adeguate tramite decisione della Commissione europea).
- Un titolare desidera utilizzare **accordi amministrativi** stipulati tra autorità pubbliche → una delle novità introdotte dal regolamento.

RESTANO VALIDE

1. **Le decisioni di adeguatezza sinora adottate** dalla Commissione;
2. gli accordi internazionali in materia di trasferimento dati stipulati prima del 24 maggio;
3. le autorizzazioni nazionali sinora emesse dal Garante successivamente a tali decisioni di adeguatezza;
4. le autorizzazioni nazionali che il Garante ha rilasciato in questi anni per specifici casi;
5. accordi e autorizzazioni fino a eventuale modifica o revisione.

È POSSIBILE TRASFERIRE I DATI VERSO PAESI TERZI

- **TRASFERIMENTO SULLA BASE DI UNA DECISIONE DI ADEGUATEZZA** SUL LIVELLO DI PROTEZIONE PRESA DALLA COMMISSIONE EUROPEA.
- **TRASFERIMENTO SOGGETTO A GARANZIE ADEGUATE** CODICI DI CONDOTTA OVVERO A SCHEMI DI CERTIFICAZIONE
- **NORME VINCOLANTI D'IMPRESA** (BCR – BINDING CORPORATE RULES)
- **DEROGHE ECCEZIONALI** PREVISTE TASSATIVAMENTE DAL LEGISLATORE EUROPEO.
  - Se l'interessato ha espressamente ed esplicitamente consentito al trasferimento, dopo essere stato informato dei possibili rischi.
  - Per importanti motivi di ordine pubblico, interessi vitali o, infine, per accertare, esercitare o difendere un diritto in sede giudiziaria.
  - Il trasferimento è necessario per l'esecuzione di un contratto a favore dell'interessato.
- **TRASFERIMENTO NON RIPETITIVO**, RIGUARDA UN NUMERO LIMITATO DI INTERESSATI ED È NECESSARIO PER IL PERSEGUIMENTO DI INTERESSI LEGITTIMI.

Al di fuori di tali situazioni ordinarie ed eccezionali, il trasferimento dei dati personali verso Paesi terzi non è mai consentito.

22

SCHEDA N. 22 – LA VALUTAZIONE DI IMPATTO - DPIA

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI DPIA

Regolamento europeo n. 2016/679 – **Art. 35**

il titolare dovrà effettuare la **valutazione d'impatto sulla protezione dei dati** (detta anche **DPIA**, acronimo del nominativo inglese "Data Protection Impact Assessment")

ogni qualvolta un tipo di trattamento preveda in particolare l'uso di nuove tecnologie, e che in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, può presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche.

OBBLIGO DI CONSULTAZIONE PREVENTIVA – Art. 36

il titolare prima di procedere al trattamento consulta inoltre l'autorità di controllo

qualora la valutazione d'impatto indichi che il trattamento presenterebbe un rischio elevato

in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

QUANDO VA EFFETTUATA?

una valutazione sistematica e globale degli aspetti personali relativi a persone fisiche, basata sul **trattamento automatizzato**, compresa la **profilazione.**

un trattamento, su larga scala, di categorie particolari di dati (**dati sensibili**), o di dati relativi a condanne penali e a reati;

operazioni di sorveglianza sistematica di zone accessibile al pubblico su larga scala.

IL CONTENUTO MINIMO DELLA DPIA

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

OBBLIGO DI CONSULTAZIONE PREVENTIVA – Art. 36

I DATI DA COMUNICARE ALL'AUTORITÀ DI CONTROLLO

IL TITOLARE DEL TRATTAMENTO COMUNICA ALL'AUTORITÀ DI CONTROLLO PER LE MOTIVAZIONI SUDDETTE ATTRAVERSO LA RICHIESTA DI CONSULTAZIONE PREVENTIVA:
→ le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;
→ le finalità e i mezzi del trattamento previsto;
→ le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;
→ i dati di contatto del titolare della protezione dei dati;
→ la valutazione d'impatto sulla protezione dei dati;
→ ogni altra informazione richiesta dall'autorità di controllo.

L'Autorità di controllo fornisce un parere scritto, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, al titolare del trattamento, se ritiene che il trattamento previsto violi il Regolamento

23 SCHEDA N. 23 – VIOLAZIONE DEI DATI – DATA BREACH

VIOLAZIONE DEI DATI – DATA BREACH

→ **Regolamento (Ue) 2016/679 –** Artt. da 32 a 34

→ prevedono una serie di adempimenti da svolgere nel caso in cui i dati personali conservati, trasmessi o trattati da aziende e Pubbliche Amministrazioni siano soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità.

→ In determinati settori vi è, infatti, l'obbligo di comunicare eventuali violazioni di dati personali **(data breach)** all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati

I DATI VIOLATI POTREBBERO AD ESEMPIO RIGUARDARE:
↘ l'**ambito finanziario**, ad esempio dati di carte di credito e di conti correnti;
↘ l'**ambito sanitario**, ad esempio informazioni sulla salute personale e malattie;
↘ **proprietà industriale**, ad esempio segreti commerciali, brevetti, documentazione riservata, lista clienti, progetti finalizzati ad esempio a pratiche di concorrenza sleale;
↘ **personali**, ad esempio dati di documenti di identità, codici personali ecc.

OBBLIGO NOTIFICA – Art.33

→ **al Garante della Privacy**

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

CONTENUTO NOTIFICA

→ descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
→ comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
→ descrivere le probabili conseguenze della violazione dei dati personali;
→ descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

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

24 SCHEDA N. 24 – VANTAGGI E INNOVAZIONI

PRINCIPALI INNOVAZIONI E NUOVE OPPORTUNITÀ

VANTAGGI

Il regolamento generale sulla protezione dei dati consente la **libera circolazione dei dati** nel **mercato unico digitale**.

proteggerà meglio la vita privata dei cittadini europei e **rafforzerà la fiducia dei consumatori e la loro sicurezza**, creando nel contempo nuove opportunità per le imprese, soprattutto quelle di piccole dimensioni.

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

VANTAGGI → **Regolamento Ue Privacy**

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

SICUREZZA

ORGANIZZAZIONE
Capacità di categorizzare i dati nei propri sistemi informatici e poterli mappare e controllare

CONTROLLO
in caso di cyber attacco (il cosiddetto data breach) è possibile identificare i dati coinvolti e adottare le misure volte a minimizzare gli effetti negativi dell'attacco.

DATA GOVERNANCE
Un sistema organizzativo e di compliance adeguato permetterà un data governance facilitato anche in grosse aziende, banche ecc.

25

SCHEDA N. 25 – SICUREZZA DEL TRATTAMENTO

SICUREZZA DEL TRATTAMENTO

Principio di sicurezza nell'art. 32 del GDPR

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

tenuto 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

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

MISURE DI SICUREZZA CHE COMPRENDONO

LA PSEUDONIMIZZAZIONE E LA CIFRATURA DEI DATI PERSONALI

LA CAPACITÀ DI ASSICURARE SU BASE PERMANENTE LA RISERVATEZZA, L'INTEGRITÀ, LA DISPONIBILITÀ E LA RESILIENZA DEI SISTEMI E DEI SERVIZI DI TRATTAMENTO

LA CAPACITÀ DI RIPRISTINARE TEMPESTIVAMENTE LA DISPONIBILITÀ E L'ACCESSO DEI DATI PERSONALI IN CASO DI INCIDENTE FISICO O TECNICO

UNA PROCEDURA PER TESTARE, VERIFICARE E VALUTARE
regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

ARTICOLO 25 REGOLAMENTO

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

ACCOUNTABILITY - RESPONSABILIZZAZIONE

26

SCHEDA N. 26 – AUTORITÀ DI CONTROLLO

AUTORITÀ DI CONTROLLO

→ **Regolamento Ue 679/2016**

→ Ogni Stato dell'Unione europea ha la sua Autorità di controllo

→ che è competente per la gestione dei reclami ad essa proposti o di eventuali violazioni del regolamento

e delle norme nazionali in materia di protezione dei dati,

AUTORITÀ DI CONTROLLO NAZIONALE ITALIANA

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

UN'AUTORITÀ AMMINISTRATIVA INDIPENDENTE ISTITUITA DALLA LEGGE SULLA PRIVACY	ESAMINA RECLAMI E SEGNALAZIONI E DECIDERE SUI RICORSI	HA IL POTERE DI IRROGARE SANZIONI

Con il nuovo regolamento europeo

→ **interviene principalmente *ex post***

cioè la sua valutazione si colloca successivamente alle valutazioni del titolare del trattamento

COMITATO EUROPEO DELLA PROTEZIONE DEI DATI

→ spetterà il ruolo di garantire uniformità di approccio alla normativa e fornire ausili interpretativi

→ e altri documenti di indirizzo sulle varie tematiche, anche per garantire gli adattamenti che si dovessero rendere necessari alla luce dello sviluppo delle tecnologie.

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

→ il titolare interpella

In via preventiva il Garante della privacy in caso di alto rischio del trattamento

27

SCHEDA N. 27 – RISK ANALISIS

RISK ANALISIS

→ **Regolamento Ue 679/2016**

→ si determinano i rischi a cui è soggetta l'organizzazione, si analizzano le vulnerabilità e si identificano le possibili salvaguardie.

→ determinare le conseguenze derivanti dal verificarsi di ciascun evento critico e di valutarne l'impatto sull'operatività dell'organizzazione.

↓ ↓

RISCHI TRATTAMENTO DEI DATI PERSONALI

- **RISCHI SIGNIFICATIVI PER I DIRITTI E LE LIBERTÀ FONDAMENTALI DELLA PERSONA**
- **RISCHIO DI DISTRUZIONE ACCIDENTALE O ILLEGALE**
- **RISCHIO DI PERDITA DEI DATI**
- **RISCHIO DI MODIFICA NON VOLUTA**
- **RISCHIO DI COMUNICAZIONE E DIFFUSIONE NON CONSENTITA**

PSEUDONIMIZZAZIONE DELLE INFORMAZIONI

→ **interviene principalmente *ex post***

↓

→ come il trattamento dei dati personali eseguito in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive.

→ informazioni aggiuntive siano **conservate separatamente**

→ NON attribuiti a una persona fisica identificata o identificabile.

→ **uso di codici e pseudonimi**

CIFRATURA DEI DATI

→ Algoritmo di cifratura e su una passphrase che "apre" e "chiude" i dati

↓

Nel Considerando n. 83 si indica proprio la cifratura delle informazioni quale sistema per mantenere la sicurezza e prevenire trattamenti in violazione al Regolamento.

Il titolare del trattamento, o il responsabile del trattamento, hanno il compito di ridurre i rischi inerenti al trattamento e attuare misure per limitare tali rischi, e tra tali misure è indicata specificamente **la cifratura**.

28 SCHEDA N. 28 – SCHEMA DI DECRETO DEL 21 MARZO

SCHEMA DI DECRETO LEGISLATIVO PER L'ADEGUAMENTO AL GDPR

→ **DECRETO LEGISLATIVO DEL 21 MARZO**

→ Il Consiglio dei Ministri ha approvato, nella seduta del 21 marzo scorso, il decreto legislativo che manda in soffitta il vecchio codice (dlgs 196/2003)

→ e introduce alcune disposizioni per adeguare la normativa italiana al Regolamento UE (GDPR) che entrerà in vigore a partire dal 25 maggio prossimo.

↓ ↓

NOVITÀ

IL CODICE DELLA PRIVACY LEGATO AL DLGS 196/2003 SARÀ ABROGATO

ABOLITI GLI ILLECITI PENALI

FARANNO SEGUITO ENTRO IL 19 MAGGIO

→ **i pareri del Consiglio di Stato**

→ i pareri delle commissioni parlamentari competenti

→ del Garante della privacy.

↓

LA DISCIPLINA SULLA PRIVACY SARÀ REGOLAMENTATA ESCLUSIVAMENTE

→ **DAL REGOLAMENTO UE**

→ **DAL DECRETO ATTUATIVO**