PRATICAMENTE PRIVACY

GDPR: novità normative e suggerimenti operativi per le imprese

CONTENUTI

Il regolamento 2016/679 in materia di protezione di dati (privacy) entrerà in vigore, salvo proroghe, il 25 maggio 2018. Nel corso dell'incontro verranno approfondite le principali novità intervenute e le implicazioni per le aziende. Verrà sviluppato il tema dell'impatto sul trattamento dei dati dei lavoratori dipendenti e collaboratori, e verranno suggeriti alcuni strumenti operativi applicabili ai casi concreti.

RELATORI

Funzionari Apindustria Confimi Vicenza
Pederzolli Alberto - Area Lavoro
Vetrugno Enrica - Area Legale

APINDUSTRIA confimiVICENZA

19 APRILE 2018 - ore 14.30

Regolamento UE 2016/679

- 4 maggio 2016: pubblicato nella Gazzetta Ufficiale dell'Unione Europea n. 119/2016
- 24 Maggio 2016: entrata in vigore
- 25 maggio 2018: applicabilità in tutti i Paesi della UE e abrogazione della direttiva 95/46/CE

APINDUSTRIA confimiVICENZA

Trattandosi di un Regolamento
e non di una Direttiva,
sarà **immediatamente applicabile**
senza necessità di recepimento
da parte degli Stati membri dell'UE.

APINDUSTRIA confimiVICENZA

Ambito di applicazione e competenza territoriale

Si applica al trattamento dei dati personali di persone fisiche e alla libera circolazione degli stessi.

E' applicato al trattamento di dati personali effettuato da un titolare o un responsabile
- stabilito nell'Unione Europea
- non stabilito nell'Unione Europea, se il trattamento ha ad oggetto dati personali di interessati che si trovano nella UE e riguarda:
  a) l'offerta di beni o servizi (anche non a pagamento) ai suddetti interessati
  b) il monitoraggio del loro comportamento nel territorio dell'Unione Europea.

Sarà possibile rivolgersi all'autorità di controllo di qualsiasi stato UE

APINDUSTRIA confimiVICENZA

La struttura del Regolamento

- CAPO I Disposizioni generali
- CAPO II Principi
- CAPO III Diritti dell'interessato
- CAPO IV Titolare e responsabile del trattamento
- CAPO V Trasferimenti di dati personali verso paesi terzi
- CAPO VI Autorità di controllo indipendenti
- CAPO VII Cooperazione e coerenza
- CAPO VIII Mezzi di ricorso, responsabilità e sanzioni
- CAPO IX Disposizioni per specifiche situazioni di trattamento
- CAPO X Atti delegati e atti di esecuzione
- CAPO XI Disposizioni finali

APINDUSTRIA confimiVICENZA

Alcune definizioni

- «**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;

APINDUSTRIA confimiVICENZA

- «**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;

- «**limitazione di trattamento**»

il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

- «**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

- «**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

APINDUSTRIA confimiVICENZA

* Attenzione *

Non esiste più una specifica definizione di

- dati personali "**sensibili**"
- dati personali "**giudiziari**"

L'art. 9 individua in generale le

- "**categorie particolari**" **di dati personali**

vale a dire le informazioni "che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona fisica".

APINDUSTRIA confimiVICENZA

I dati

L'art. 5 del Regolamento stabilisce che:

• devono essere **trattati** in modo **lecito, equo e trasparente** nei confronti dell'interessato

• devono essere raccolti per **finalità determinate, esplicite e legittime**, e successivamente trattati in modo non incompatibile con tali finalità

I tempi di conservazione dei dati personali devono:

• essere commisurati e non eccedenti rispetto alle finalità
• tenere conto di eventuali prescrizioni di Legge

Il titolare del trattamento dovrebbe stabilire un
termine per la cancellazione o
per la **verifica periodica**

APINDUSTRIA confimiVICENZA

Soggetti coinvolti

Obblighi organizzativi nuovi con riferimento ai loro ruoli e funzioni:

1. nel caso di **contitolarità del trattamento**,

quando due o più titolari del trattamento determinano insieme le finalità e i mezzi del trattamento, va redatto uno specifico accordo interno tra i contitolari che disciplini in modo trasparente le rispettive responsabilità e rifletta adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo va messo a disposizione dell'interessato;

2. con riferimento al **Responsabile del trattamento**,

la sua nomina va documentata con un "*contratto o altro atto giuridico*"- stipulato in forma scritta o anche in formato elettronico - che regoli 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.

APINDUSTRIA confimiVICENZA

3. il Responsabile del trattamento può a sua volta designare
Sub-responsabili del trattamento

ma previa autorizzazione scritta, specifica o generale, del titolare del trattamento;

4. gli incaricati del trattamento non sono menzionati nel Regolamento, che però prevede la figura delle

Persone autorizzate al trattamento

soggetti che operano sotto la diretta responsabilità del titolare o del responsabile con apposite istruzioni (sembrerebbero restare in vigore le obbligatorie istruzioni agli incaricati, anche se il Regolamento non prevede nulla riguardo alla forma scritta);

5. il **Rappresentante del titolare del trattamento**

stabilito nella UE va designato per iscritto in caso di trattamenti effettuati da titolari non stabiliti nella UE se il trattamento ha ad oggetto dati personali di interessati che si trovano nella UE e riguarda
1) l'offerta di beni o servizi (anche non a pagamento) ai suddetti interessati
2) il monitoraggio del loro comportamento nel territorio dell'Unione Europea.

Titolare del trattamento

A) determina realmente le finalità e i mezzi del trattamento

B) adotta politiche e attua misure adeguate ed efficaci per tutelare i diritti e le libertà dell'interessato, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche

C) deve essere in grado di dimostrare l'efficacia delle misure e la conformità delle attività di trattamento con il regolamento.

Data Protection Officer (DPO) = Responsabile Protezione Dati (RPD) Art. 37

E' designato dal titolare del trattamento e dal responsabile del trattamento solo se:

1. il trattamento è effettuato da **un'autorità pubblica** o da **un organismo pubblico** (eccettuate le autorità giurisdizionali)

2. le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che 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 dati particolari (personali sensibili, sanitari, sulla vita o sull'orientamento sessuale, genetici, biometrici, o di dati relativi a condanne penali e a reati).

Il DPO va designato in funzione delle elevate qualità professionali e della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati.

APINDUSTRIA confimiVICENZA

Un **gruppo** imprenditoriale **può nominare un unico** DPO, a condizione che sia facilmente raggiungibile da ciascuno stabilimento.
Il DPO **può essere un dipendente,** soggetto interno alla struttura, del Titolare del trattamento o del responsabile del trattamento oppure **un Soggetto esterno** che assolve i suoi compiti in base a un **contratto di servizi**.
I **dati di contatto** del Data Protection Officer vanno **comunicati al Garante e resi pubblici**.
Va coinvolto in tutte le questioni riguardanti la protezione dei dati personali e deve avere le risorse necessarie per assolvere ai compiti assegnati.
Non deve ricevere alcuna istruzione per quanto riguarda l'esecuzione dei compiti affidati (è figura del tutto autonoma) **né è soggetto a potere disciplinare o sanzionatorio** per l'adempimento dei propri compiti.

APINDUSTRIA confimiVICENZA

Funzioni
Art. 39

Il **nucleo minimo** (che dunque può essere anche esteso) dei compiti assegnati al Responsabile della protezione dei dati:

• Informare e consigliare il titolare, il responsabile o i dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento

• Sorvegliare l'osservanza del Regolamento

• Fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento

• Cooperare e fungere da punto di contatto con l'autorità di controllo

Principi

- *Accountability*: responsabilizzazione del titolare
- *Privacy by design* e *privacy by default*
- *Trasparenza:* informativa e consenso

APINDUSTRIA confimiVICENZA

Accountability
Art. 24 - 25

Il Titolare è il soggetto competente a **garantire** il rispetto dei principi di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza dei dati (art. 5).

Il Titolare **deve essere in grado di "comprovarlo"** (principio di "accountability"), ha l'onere di porre in essere una serie di adempimenti (tra cui la mappatura delle operazioni di trattamento mediante la creazione di un apposito registro) che rendano i principi posti dalla nuova disciplina dati verificabili nei fatti e non più soltanto obblighi giuridici esistenti sulla carta.

Il Titolare del trattamento quindi **assicura e comprova** che ciascuna operazione di trattamento di dati personali sia conforme al Regolamento.

APINDUSTRIA confimiVICENZA

Il Titolare del trattamento deve **mettere in atto** (nonché riesaminare ed aggiornare se necessario) **misure tecniche ed organizzative adeguate** per garantire, ed essere in grado di dimostrare, che le operazioni di trattamento vengano effettuate in conformità alla nuova disciplina.

Le misure da adottare vanno valutate di volta in volta, tenendo in considerazione una serie di elementi tra cui la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, nonché i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Non sono previste "misure minime" da adottare, ma è necessario individuare di volta in volta **misure maggiormente adeguate**, alla luce degli elementi sopra indicati.

APINDUSTRIA confimiVICENZA

SICUREZZA

Riservatezza: accessibile solo a chi è autorizzato, non accessibile a chi non è autorizzato

Integrità:corretto, aggiornato, non corrotto o "falsificato"

Disponibilità: agevolmente disponibile a chi vi può lecitamente accedere

APINDUSTRIA confimiVICENZA

Eventi che causano la perdita di sicurezza

- Rottura di un hard disk
- Virus
- Assenza di password
- Profili mal configurati
- Perdita di chiavetta USB
- Furto di PC
- Assenza dell'incaricato
- Comunicazione di password
- Furto di documenti
- Pubblicazione illecita su Internet
- Accesso non autorizzato a dati giudiziari
- Sostituzione di un PC
- Dimissioni di un dipendente
- Introduzione di un nuovo server
- Attivazione di collegamento remoto
- Introduzione di un nuovo programma applicativo
- Nuova normativa
- Violazione di dati
- Nuova vulnerabilità software e hardware
- Nuova versione di un sistema operativo

APINDUSTRIA confimiVICENZA

privacy by design

Il titolare del trattamento - 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 – deve:

- applicare misure tecniche e organizzative adeguate (es: anonimizzazione) volte ad attuare in modo efficace i principi di protezione dei dati e
- integrare nel trattamento le necessarie garanzie per tutelare i diritti degli interessati

Tale adempimento va effettuato sia al momento di determinare i mezzi del trattamento (es: progettazione di *device*) sia all'atto del trattamento stesso.

APINDUSTRIA confimiVICENZA

Il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire che siano **trattati, per impostazione predefinita** (cioè di *default*), **solo i dati personali necessari** per ogni specifica finalità del trattamento.
Tale obbligo vale per la quantità dei dati personali raccolti, l'estensione del trattamento, il periodo di conservazione e la loro accessibilità.

In particolare, dette misure devono garantire che, per impostazione predefinita, **non siano resi accessibili dati personali a un numero indefinito di persone** fisiche senza l'intervento della persona fisica (che ad esempio consapevolmente disponga il settaggio dell'apparato o del servizio scegliendo di condividere con i terzi i dati personali oggetto di trattamento nell'ambito della operatività dell'apparato o del servizio).

APINDUSTRIA confimiVICENZA

Trasparenza

Per le persone fisiche dovrebbero essere trasparenti

- le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano
- la misura in cui i dati personali sono o saranno trattati.

Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro.

APINDUSTRIA confimiVICENZA

Informativa

Gli interessati dovranno sapere se i loro dati sono trasmessi al di fuori dell'Ue e con quali garanzie; cosi come dovranno sapere che hanno il diritto di revocare il consenso a determinati trattamenti, come quelli a fini di marketing diretto.

Il Titolare del trattamento ha **obblighi di informativa** prevedendo **numerose informazioni aggiuntive** da fornire agli interessati. L'Informativa **va resa per iscritto o con altri mezzi, anche elettronici**.

Se richiesto dall'interessato, le informazioni possono essere fornite **oralmente**, purché sia comprovata con altri mezzi l'identità dell'interessato.

APINDUSTRIA confimiVICENZA

Informazioni aggiuntive obbligatorie 1

1. dati di contatto del Titolare, del Responsabile del trattamento e del Responsabile della protezione dei dati personali

2. finalità e base giuridica del trattamento

3. qualora il trattamento si basi sulla necessità di perseguire un legittimo interesse del Titolare del trattamento o di terzi, la specificazione di quali siano i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

4. gli eventuali destinatari dei dati personali;

5. l'intenzione di trasferire dati personali a un paese terzo o a un'organizzazione internazionale;

6. il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

7. 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

APINDUSTRIA confimiVICENZA

Informazioni aggiuntive obbligatorie 2

8. l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca

9. il diritto di proporre reclamo al Garante privacy

10. se la comunicazione di dati personali è un obbligo o un requisito necessario per la conclusione di un contratto e se l'interessato ha l'obbligo di fornirli nonché le conseguenze della mancata comunicazione di tali dati

11. l'eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato

12. informare l'interessato, prima del trattamento, se si intende trattare i dati personali per una finalità diversa da quella per cui essi sono stati raccolti

APINDUSTRIA confimiVICENZA

Informazioni aggiuntive obbligatorie 3

Se i dati non sono stati ottenuti presso l'interessato, il Titolare del trattamento fornisce anche le seguenti informazioni:

1. la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico

2. le categorie di dati personali oggetto del trattamento

3. l'obbligo di fornire le informazioni all'interessato entro un mese dall'ottenimento dei dati o alla prima comunicazione se destinati alla comunicazione con l'interessato, oppure non oltre la prima comunicazione se è prevista la comunicazione ad altro destinatario

APINDUSTRIA confimiVICENZA

E' la BASE del trattamento dei dati
e deve sempre essere fornita all'interessato

E' un presupposto fondamentale per la validità del consenso

Può esistere senza consenso, ma
NON
si può avere un consenso
che non preceduto da idonea informativa.

APINDUSTRIA confimiVICENZA

Consenso

Principale precondizione (salvo le deroghe) di liceità del trattamento.

Espresso mediante un **atto positivo inequivocabile** con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio **mediante dichiarazione scritta,** anche attraverso **mezzi elettronici, o orale**.

E' vietato trattare «categorie particolari di dati personali» a meno che l'interessato non abbia prestato il proprio **consenso esplicito** o nei casi indicati dall'art. 9.

APINDUSTRIA confimiVICENZA

Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità; qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste.

Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.

Il Titolare del trattamento deve poter dimostrare che l'interessato ha prestato il consenso al trattamento dei propri dati personali.

Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve **essere presentata in modo chiaramente distinguibile dalle altre materie**, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro, **pena l'invalidità del consenso prestato**.

APINDUSTRIA confimiVICENZA

L'interessato ha il
diritto di revocare il proprio consenso
(tale informazione è uno dei
nuovi elementi obbligatori dell'informativa)
in qualsiasi momento
(anche se la revoca non pregiudica la
liceità del trattamento fino a quel momento
effettuato),
con modalità di esecuzione della revoca del consenso
facili come la sua prestazione originaria.

APINDUSTRIA confimiVICENZA

I diritti dell'interessato

- alla **trasparenza** del trattamento
- all'**accesso** ai dati
- alla **rettifica** dei dati
- alla **limitazione** del trattamento
- all'**opposizione** al trattamento
- all'**oblio**
- alla **portabilità** dei dati
- al **risarcimento del danno**

APINDUSTRIA confimiVICENZA

Limitazione di trattamento e opposizione al trattamento
Art. 18

Diritto alla limitazione di trattamento:
nei casi tassativamente previsti dal Regolamento stesso, i dati sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Diritto di opposizione al trattamento:
in base alla sua situazione particolare, ciascun soggetto può infatti opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano, in special modo quando i dati sono trattati per **finalità di marketing diretto**.

APINDUSTRIA confimiVICENZA

* Attenzione *

Per una tutela effettiva, l'interessato può:

- **proporre reclamo** all'autorità di controllo dello Stato in cui risiede ogni qual volta ritenga che i propri dati vengano trattati in violazione al Regolamento 679/2016.
Se entro tre mesi dal reclamo l'autorità di controllo non si esprime sull'esito o sullo stato del reclamo, l'interessato ha il diritto di
- proporre un **ricorso giurisdizionale effettivo nei confronti di tale autorità di controllo** di fronte agli organi giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita.

- proporre un ricorso giurisdizionale direttamente nei confronti del titolare o del responsabile del trattamento qualora l'interessato ritenga che i diritti di cui gode a norma del Regolamento siano stati da loro violati a seguito di operazioni di trattamento.

Tali azioni possono essere promosse di fronte agli organi giurisdizionali dello Stato membro in cui il titolare ha uno stabilimento ovvero dello Stato in cui risiede l'interessato.

APINDUSTRIA confimiVICENZA

Diritto all'oblio
Art. 17

Diritto alla cancellazione dei dati senza ingiustificato ritardo espressamente se:

- i dati non sono più necessari rispetto alle finalità per cui erano stati raccolti o trattati;
- l'interessato revoca il consenso e non sussiste altro fondamento giuridico per il trattamento;
- l'interessato si oppone al trattamento e non sussiste altro fondamento giuridico per continuare lo stesso;
- i dati sono stati trattati illecitamente;
- i dati devono essere cancellati per legge;
- i dati sono stati forniti da un minore.

Se il Titolare del trattamento ha reso pubblici i dati oggetto di richiesta di cancellazione, è obbligato, tenendo conto della tecnologia disponibile e dei costi di attuazione, anche ad avvertire tutti i soggetti che trattano tali dati di cancellare qualsiasi link, copia o riproduzione di essi.

Diritto alla portabilità
Art. 20

Diritto di **trasferire i dati da un titolare ad un altro**.

A condizione che il trattamento si basi sul consenso o su un contratto e che non vengano lesi diritti e libertà altrui.

Se tecnicamente fattibile, la trasmissione deve essere fatta direttamente da un titolare all'altro.

Per rendere il tutto effettivamente possibile, è previsto il diritto per l'interessato di ricevere i propri dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico.

Sarà quindi un diritto di ciascuno di noi cambiare ad es. provider di posta elettronica mantenendo tutti i contatti e tutti i messaggi di posta salvati

APINDUSTRIA confimiVICENZA

Diritto al risarcimento del danno
Art. 82

Chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal Titolare del trattamento o dal Responsabile del trattamento.

APINDUSTRIA confimiVICENZA

... 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 ...

APINDUSTRIA confimiVICENZA

Le misure di sicurezza nel trattamento dei dati personali
Art. 32

Il Titolare del trattamento e il Responsabile del trattamento debbano mettere in atto Misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre:

1. la **pseudonimizzazione** e la **cifratura** dei dati personali;

2. la capacità di **assicurare su base permanente** la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

3. la capacità di **ripristinare tempestivamente la disponibilità e l'accesso** dei dati personali in caso di incidente fisico o tecnico;

4. una **procedura per testare, verificare e valutare regolarmente l'efficacia delle misure** tecniche e organizzative al fine di garantire la sicurezza del trattamento.

APINDUSTRIA confimiVICENZA

Obbligo di documentazione delle misure di sicurezza (analogo al DPS):

a) obbligo di inserire nel *Registro delle attività di Trattamento* la "descrizione generale delle misure di sicurezza tecniche e organizzative"

b) obbligo di inserire nella V*alutazione preventiva di impatto sulla protezione dei dati*, la "descrizione delle misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone"

APINDUSTRIA confimiVICENZA

La notifica della violazione dei dati personali

DATA BREACH

violazione della 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

Il Titolare del trattamento notifica la violazione al Garante 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 non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

APINDUSTRIA confimiVICENZA

Contenuti della notifica

1. **natura della violazione** dei dati 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

2. **nome e i dati di contatto del Responsabile della protezione dei dati (DPO)** o di altro punto di contatto presso cui ottenere più informazioni

3. **probabili conseguenze della violazione**

4. **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.

APINDUSTRIA confimiVICENZA

* Attenzione *

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento
comunica la violazione anche all'interessato,
senza ingiustificato ritardo,
descrivendola con un linguaggio semplice e chiaro
(salve circostanze al verificarsi delle quali non è richiesta la comunicazione).

APINDUSTRIA confimiVICENZA

Trasferimento dei dati fuori dell'Unione Europea

1. trasferimento sulla base di una decisione di adeguatezza

ove la Commissione UE abbia deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato; in tal caso il trasferimento non necessita di autorizzazioni specifiche

2. trasferimento soggetto a garanzie adeguate

il Titolare del trattamento o il Responsabile del trattamento può trasferire dati personali verso un Paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate, come ad esempio le norme vincolanti d'impresa, le clausole contrattuali standard, l'esistenza di un codice di condotta, l'esistenza di un meccanismo di certificazione, specifiche clausole contrattuali

APINDUSTRIA confimiVICENZA

Se non è applicabile nessuna delle condizioni prima illustrate il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale sono ammessi soltanto se si verifica una delle seguenti condizioni:

a) il consenso informato dell'interessato;
b) il trasferimento è necessario all'esecuzione di un contratto ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;
c) il trasferimento sia necessario per importanti motivi di interesse pubblico o per accertare, esercitare o difendere un diritto in sede giudiziaria;
d) il trasferimento sia 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;
e) il trasferimento sia effettuato a partire da un registro pubblico.

APINDUSTRIA confimiVICENZA

Privacy Impact Assessment (PIA): valutazione d'impatto sulla protezione dei dati Art. 35

Quando il trattamento (per natura, oggetto, contesto e finalità), in particolare se prevede l'uso di nuove tecnologie, presenta un **rischio elevato** per i diritti e le libertà degli interessati, il titolare del trattamento effettua una **valutazione d'impatto**, del trattamento previsto, sulla protezione dei dati personali per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio.

L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento.

Laddove la valutazione d'impatto sulla protezione dei dati indichi che i **trattamenti presentano un rischio elevato** che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe **consultare l'autorità di controllo**.

APINDUSTRIA confimiVICENZA

Richiesta in particolare nei seguenti casi:

• valutazione sistematica e globale di aspetti della personalità dell'interessato o volta ad analizzarne o prevederne in particolare la situazione economica,l'ubicazione, lo stato di salute, le preferenze personali, l'affidabilità o il comportamento, basata su un trattamento automatizzato e da cui discendo misure che hanno effetti giuridici o significativamente incidono sull'interessato;

• il trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9, o di dati relativi a condanne penali e a reati di cui all'art. 10;

• **la sorveglianza sistematica su larga scala di una zona accessibile al pubblico**.

APINDUSTRIA confimiVICENZA

Contenuti minimi

• descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso l'interesse legittimo perseguito dal Titolare del trattamento (ove applicabile)
• valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
• valutazione dei rischi per i diritti e le libertà degli interessati;
• misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il titolare del trattamento, prima di procedere al trattamento, consulta 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.
Il titolare trasmesse all'autorità di controllo la valutazione d'impatto e tutte le altre informazioni richieste.

APINDUSTRIA confimiVICENZA

Sanzioni

Responsabilità risarcitoria per il c.d. "*danno da trattamento*":

"*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*" (Art. 82).

Ripartizione della responsabilità risarcitoria tra titolare e responsabile del trattamento, e tra contitolari del trattamento, con previsione specifica di azioni di regresso reciproche.

Meccanismi di esonero.

APINDUSTRIA confimiVICENZA

Sanzioni amministrative pecuniarie
Art. 83

1. fino a **10.000.000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore, nel caso di violazione di determinati obblighi posti dal Regolamento;

2. fino a **20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore, nel caso di violazione degli obblighi più stringenti posti dal Regolamento (anche nel semplice caso di inosservanza degli ordini del Garante.

APINDUSTRIA confimiVICENZA

Divieto di trattamento
Art. 58

Tra i **poteri correttivi** delle Autorità di controllo è prevista la possibilità di limitare o vietare un trattamento.
Le conseguenze economiche di una disposizione di questo tipo potrebbero essere anche più gravi di quelle derivanti da una sanzione amministrativa.
L'impossibilità di effettuare un trattamento potrebbe comportare, ad esempio, la sospensione dell'erogazione di un servizio verso i clienti.

APINDUSTRIA confimiVICENZA

Adempimenti

I principali adempimenti riguardano:

a)l'organizzazione interna dell'impresa

b)i rapporti con i fornitori esterni

c)la revisione della modulistica con i clienti/utenti

d)la programmazione e l'attuazione del sistema di sicurezza nella protezione dei dati

e)la predisposizione della documentazione per dimostrare la propria conformità alle regole

f)la formazione del personale

g)l'eventuale adesione a codici di correttezza e a sistemi di certificazione

APINDUSTRIA confimiVICENZA

a) Organizzazione interna

I Soggetti Autorizzati al trattamento (ex «incaricati») devono ricevere istruzioni e formazione da parte del Titolare del trattamento.

Ci sono soggetti apicali (figure NON obbligatorie) che si chiamano Responsabili interni del trattamento.

Una figura a sé stante è il Responsabile della Protezione dei dati (RPD) = DPO (Data Protection Officer) (figura obbligatoria SOLO in alcuni casi), può (anzi, si consiglia) essere un soggetto esterno

APINDUSTRIA confimiVICENZA

b) rapporti con i fornitori esterni

Possono essere previsti i Responsabili esterni, che trattano dati per conto del Titolare del trattamento (figure NON obbligatorie ai fini privacy, ma sovente obbligatorie per Legge)

Lo strumento del contratto deve essere utilizzato per regolare i rapporti tra Titolare e Responsabile del trattamento (SI anche a contratto quadro con possibilità per Responsabile di nominare Sub-Responsabili)

APINDUSTRIA confimiVICENZA

Rapporto con clienti / utenti

Il Titolare del trattamento deve:

-dare un'idonea informativa

-verificare a quali condizioni può trattare i dati (cd. LICEITA' DEL TRATTAMENTO)

APINDUSTRIA confimiVICENZA

Per i dati comuni ci sono 6 possibilità:

1.Consenso

2.esecuzione del contratto o di misure precontrattuali

3.Adempimento di un obbligo di Legge

4.Salvaguardia di interessi vitali

5.Esecuzione di un compito di interesse pubblico

6.Perseguimento del legittimo interesse del Titolare purchè non sovrasti quello dell'Interessato

Per i dati particolari le possibilità sono 10:

1.Consenso esplicito

2.Necessità di assolvere obblighi in materia di diritto del lavoro e sicurezza sociale

3.Tutela di un interesse vitale dell'interessato

4.Trattamento in ambito delle legittime attività (associazioni etc.)

5.Trattamento di dati resi manifestamente pubblici

6.Accertamento di un diritto in sede giudiziaria

7.Motivi di interesse pubblico

8.Finalità di medicina pubblica e/o del lavoro

9.Minacce per la salute

10.Archiviazione e ricerca scientifica

Consenso

Deve essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, inequivocabile e informata di accettare il trattamento dei dati

SI dichiarazione scritta
SI mezzi elettronici
SI orale (ma attenzione alla prova)

Responsabilità e sanzioni

Responsabilità in caso di mancato adempimento al Reg.
A)Civile per danni
B)Connessa all'esercizio dei diritti da parte dell'interessato

In tema di responsabilità civile, chiunque subisca un danno materiale o immateriale causato da una violazione del Reg. ha diritto al risarcimento del danno dal Titolare del trattamento o dal Responsabile del trattamento (se ha agito in modo difforme dalle istruzioni o non ha adempiuto agli obblighi suoi propri)

L'onere della prova è a carico del presunto autore della violazione: Titolare o Responsabile sono esonerati se dimostrano che il fatto non gli è in alcun modo imputabile.

E' solidale, salvo rivalsa nei limiti della quota di responsabilità.

Le sanzioni sono PESANTI, ma c'è modo di adeguarle AL CASO CONCRETO, e sarà compito del Garante.

Ai sensi dell'art. 58 Reg. il Garante ha il potere di:

-Rivolgere avvertimenti al Titolare o al Responsabile sul fatto che il trattamento possa verosimilmente violare le disposizioni

-Rivolgere ammonimenti se il trattamento ha violato le disposizioni

Come fare per mettersi in regola

La norma CHIAVE del Reg. è l'art. 5 paragrafo 2

Due precetti:

1.Attribuzione al Titolare del trattamento del compito di attuare gli adempimenti previsti dalla normativa (in negativo, individuazione nel Titolare del soggetto cui comminare le violazioni)

2.Assegnazione al Titolare del trattamento dell'onere di provare l'avvenuto adeguamento alla normativa

APINDUSTRIA confimiVICENZA

L'onere della prova si realizza attraverso il confezionamento di un «**DOSSIER PRIVACY**» che costituisce il CORPO = conformità dell'adeguamento al Reg. (cd. COMPLIANCE)

La documentazione delle scelte consente al Titolare di dimostrare perché si è comportato in un certo modo e questo è un elemento utile di prova in caso di contestazioni.

APINDUSTRIA confimiVICENZA

Adempimenti e documenti

1) Mappa trattamenti : REGISTRO TRATTAMENTI

2) Sicurezza: a) esecuzione misure tecniche : DOCUMENTO VALUTAZIONE DEI RISCHI

b) verifica obblighi di compilazione (anche DPO) ed esecuzione misure tecniche ed organizzative : DOCUMENTO VALUTAZIONE D'IMPATTO

c) individuazione ufficio responsabile, compilazione protocollo di azioni, verifica cause esonero : DATA BREACH

3) Contitolari: stesura e sottoscrizione accordo : ACCORDO

APINDUSTRIA confimiVICENZA

4) Nomine Responsabili esterni: mappatura dell'outsourcing dei dati, compilazione contratti, esecuzione misure normative, tecniche ed organizzative previste in contratto : CONTRATTO DI RESPONSABILE ESTERNO

5) Nomine Sub – Responsabili esterni: mappatura dati, regolarizzazione o stesura contratti : CONTRATTO CON SUB – RESPONSABILI

6) Nomine Responsabili interni: mappature nomine esistenti, aggiornamento a nuovi compiti : ATTO DI NOMINA E DISCIPLINARE

APINDUSTRIA confimiVICENZA

7) Nomine Autorizzati: mappatura nomine esistenti, verifiche di adeguamento, profili utente, aggiornamento nuovi compiti : NOMINE DIPENDENTI E COLLABORATORI

8) Formazione Autorizzati: corsi di livello diverso (anche appositi per candidati DPO interni) : CORSI PER GLI AUTORIZZATI

9) Rapporti con gli interessati: a) verifica informative esistenti, allineamento ai nuovi contenuti, eventuali abbinamento a icone (videosorveglianza)

b) verifica consensi esistenti, allineamento : INFORMATIVA

APINDUSTRIA confimiVICENZA

10) RDP = DPO: verifica obbligo/opportunità di nomina, scelta del professionista/organizzazione esterna, stesura e sottoscrizione contratto, esecuzione misure previste in contratto : NOMINA RDP/DPO E POLICY INTERNA

11) Trasferimenti dati estero - Extra UE: verifica e rispetto delle condizioni di liceità (es. codici di condotta del destinatario, certificazioni, clausole contrattuali, legittimo interesse etc.) : CONDIZIONE DI LICEITA'

12) Certificazioni: acquisizione, esecuzione misure di mantenimento : CERTIFICAZIONE *

APINDUSTRIA confimiVICENZA

13) Codice di condotta: adesione, esecuzione misure di mantenimento : CODICE DI CONDOTTA

APINDUSTRIA confimiVICENZA