CORSO DI AGGIORNAMENTO FORMATIVO

IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

ai sensi del Regolamento (UE) 2016/679 GDPR

MARTEDI' 25 FEBBRAIO 2024 ORE 14,30 – 16,00

REGOLAMENTO UE 2016/679 - GDPR

REGOLAMENTO EUROPEO 2016/679

E' un regolamento con il quale la Commissione Europea intende rafforzare e rendere più omogenea la protezione dei dati personali di cittadini dell'Unione Europea e dei residente nell'Unione Europea, sia all'interno che all'esterno dei confini della stessa UE. Il testo pubblicato su Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno, è diventato applicabile il 25 maggio 2018 dopo un periodi di tranzione di 2 anni.

Ha in generale l'obiettivo di proteggere i diritti e le libertà delle persone fisiche in ordine al trattamento dei dati personali

Successivamente è stato pubblicato il D.Lgs 10 agosto 2018 n. 101, entrato in vigore il 19/09/2018, che ha armonizzato la normativa italiana a quella europea.

Con tale Regolamento, l'azienda è “responsabilizzata” ad analizzare la propria situazione e gli eventuali specifici rischi per poi porre in essere azioni concrete anche a livello organizzativo.

Cosa si intende per DATO PERSONALE

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

CATEGORIE PARTICOLARI DI DATI PERSONALI (ex sensibili)
Qualsiasi informazione che riveli l'origine razziale o etnica; le opinioni politiche; le convinzioni religiose o filosofiche; l'appartenenza sindacale; dati genetici, biometrici intesi a identificare in modo univoco una persona fisica; dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

DATI GIUDIZIARI
Sono quelli relativi a Condanne penali e a reati o a connesse misure di sicurezza. Rivelano l'esistenza di provvedimenti penali suscettibili di iscrizione nel casellario giudiziale, oppure la qualità di indagato o imputato.

Cosa si intende per TRATTAMENTO

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

I PRINCIPI DEL GDPR

A Accountability

L'impresa deve dimostrare la conformità al GDPR delle proprie attività, 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*" (GDPR C74).

L'*accountability* consiste in una sostanziale **responsabilità generalizzata** del titolare per tutto ciò che attiene alla protezione dei dati personali.

Si tratta di un principio cardine dell'intero GDPR che innerva tutti gli aspetti della tutela della privacy, quali ad esempio: la valutazione del rischio, la tenuta del registro dei trattamenti, l'identificazione dei ruoli privacy all'interno dell'azienda e l'adozione delle misure tecnico – organizzative.

I PRINCIPI DEL GDPR

B Principi di legittimità del trattamento

L'impresa deve effettuare il trattamento di dati personali osservando i principi di legittimità indicati nel GDPR (artt. 5 – 11)

Liceità/base giuridica: il trattamento è lecito se ricorre almeno una della seguenti condizioni:
- consenso dell'interessato
- adempimento di obblighi contrattuali
- obbligo legale cui è soggetto il titolare
- esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento

Finalità: l'impresa può trattare i dati personali solo per finalità determinate, esplicite e legittime, che devono essere indicate nell'informativa resa all'interessato. Di conseguenza, ogni finalità diversa, sorta in un momento successivo alla raccolta dei dati necessita di una nuova informativa

I PRINCIPI DEL GDPR

B1 CONSENSO

Definizione di consenso: art. 4 GDPR

"(...)qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positive inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Il consenso è una delle basi giuridiche del trattamento dei dati (= ciò che autorizza legalmente il trattamento)

[2] Per la descrizione dell'interesse legittimo del titolare si veda più avanti il focus n. 3.

I PRINCIPI DEL GDPR

Minimizzazione: l'impresa può trattare solo i dati personali adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità individuate.

Esattezza: l'impresa deve assicurarsi che i dati personali siano esatti e aggiornati e, in caso contrario, correggerli.

Conservazione: l'impresa deve garantire che i dati personali siano conservati per un periodo non superiore a quello necessario agli scopi per i quali sono stati raccolti.

Integrità e riservatezza: l'impresa deve predisporre adeguate misure tecniche e organizzative che garantiscano la sicurezza dei dati personali, compresa la protezione contro il trattamento non autorizzato o illecito e contro la perdita accidentale, la distruzione o il danno, utilizzando tecnologie appropriate.

C Protezione dei dati by design e by default

L'impresa deve tenere in considerazione il principio di protezione dei dati personali fin dalle prime fasi della progettazione delle attività di trattamento e per tutto il ciclo di vita del dato. Deve, inoltre, costruire un efficiente sistema di protezione dei dati personali che, di *default*, consenta di minimizzare la quantità di dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità dei dati stessi (tenuto conto dei costi di attuazione, della natura, del contesto e delle finalità del trattamento, nonché dei rischi di diversa gravità come previsto da GDPR art. 25).

Privacy by design

L'impresa, fin dalla fase di progettazione, deve mettere in atto misure tecniche e organizzative che consentano, ad esempio, di:

- raccogliere solo i dati personali strettamente necessari;
- limitare la diffusione dei dati personali;
- garantire il ripristino dei dati in caso di danneggiamento o malfunzionamento del sistema informativo;
- effettuare una periodica cancellazione dei dati personali non più necessari.

Privacy by default

L'impresa deve fare in modo che le misure a tutela della privacy si attivino, per quanto possibile, in maniera automatica quando vi è un trattamento di dati personali. L'impresa dovrà in particolare impostare, di default, nel modo meno invasivo possibile per la privacy delle persone interessate, i seguenti elementi:

Quantità dei dati raccolti – l'impresa deve valutare sia la quantità dei dati raccolti sia la pertinenza dei dati per le finalità di trattamento perseguite. L'impresa deve limitare la portata del trattamento ed evitare di effettuare un trattamento eccedente di dati personali, qualora ciò non sia necessario per fornire il servizio/il prodotto.

Periodo di conservazione – l'impresa deve impostare tempi di conservazione che siano più ridotti possibile senza, tuttavia, pregiudicare il raggiungimento delle finalità perseguite.

Accessibilità – l'impresa deve adottare misure per garantire la protezione dei dati per impostazione predefinita che assicurino che i dati personali non siano resi accessibili a un numero indefinito di persone fisiche senza l'intervento dell'interessato (ad es. impostando livelli di accesso differenziati a dipendenti e collaboratori a seconda delle necessità e delle finalità del trattamento).

ADEMPIMENTI NECESSARI PER LA COMPLIANCE: LE MISURE TECNICO - ORGANIZZATIVE

Ai sensi dell'art. 32 del GDPR, l'impresa è tenuta ad adottare misure tecnico - organizzative che garantiscano un livello di sicurezza adeguato al rischio, sulla base: dei trattamenti svolti in concreto e delle caratteristiche della propria organizzazione.

Al fine di valutare tali aspetti e, conseguentemente, definire il livello di rischio in cui ciascuna impresa si colloca, l'impresa deve valutare i molteplici aspetti della conformità al GDPR, individuando le eventuali misure necessarie, sia a livello organizzativo (formazione, modulistica, nomina dei responsabili del trattamento ove necessario, istruzioni ai soggetti autorizzati etc.) sia a livello tecnico (sicurezza informatica, sicurezza fisica, sicurezza dei dati trattati con modalità cartacee, etc.).

ADEMPIMENTI NECESSARI PER LA COMPLIANCE: LE MISURE TECNICO - ORGANIZZATIVE

A Misure organizzative

1. Formazione

L'impresa deve prevedere ed organizzare la formazione sia per i vertici aziendali (imprenditore, soci e *management*) sia per i dipendenti.

La formazione si articola nei seguenti livelli:

Formazione sui contenuti generali del GDPR (tra cui: principi di protezione dei dati personali, *privacy by design e by default*, minimizzazione, responsabilizzazione, misure di sicurezza).

Formazione specifica – L'impresa deve prevedere una specifica formazione per i dipendenti/addetti che trattano dati personali affinché siano chiare le finalità, i limiti e le modalità del trattamento stesso.

Aggiornamento periodico – L'impresa deve prevedere un periodico aggiornamento della formazione degli addetti al trattamento. La frequenza dell'aggiornamento è stabilita dall'impresa sulla base del rischio dell'attività svolta.

Formazione sull'uso degli strumenti/dispositivi informatici di lavoro – L'impresa deve fornire al dipendente/collaboratore norme sul corretto uso aziendale e sulle responsabilità per uso improprio del telefono, dei dispositivi informatici e dei supporti esterni (ad es. stampanti).

FORMAZIONE IN AZIENDA IN MATERIA DI TRATTAMENTO DI DATI PERSONALI

Il Regolamento (Ue) 2016/679 in materia di trattamento dei dati personali (GDPR) affida all'impresa il compito di adottare misure tecnico - organizzative che garantiscano un livello di sicurezza adeguato al rischio, sulla base:
dei trattamenti svolti in concreto e
delle caratteristiche della propria organizzazione.
Tra le misure organizzative che l'impresa deve adottare rientra certamente la formazione del titolare dell'azienda e dei suoi dipendenti.
Il GDPR, infatti, in diversi articoli affida alle figure chiave della gestione della privacy in azienda (titolare, responsabile del trattamento e data protection officer-DPO) compiti specifici:
il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento*, che abbia accesso a dati personali* ***non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento****, salvo che lo richieda il diritto dell'Unione o degli Stati membri* (artt. 28 e29);
il titolare del trattamento e il responsabile del trattamento *fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali* ***non tratti tali dati se non è istruito in tal senso dal titolare del trattamento****, salvo che lo richieda il diritto dell'Unione o degli Stati membri* (art. 32);

FORMAZIONE IN AZIENDA IN MATERIA DI TRATTAMENTO DI DATI PERSONALI

A Formazione generale

La formazione generale **è obbligatoria per tutto il personale che tratta dati personali** in azienda (ad esempio addetti alle risorse umane, al marketing, all'amministrazione, alla gestione di clienti e fornitori).

Sono, invece, esclusi dall'obbligo formativo coloro che non effettuano trattamenti di dati personali come, ad esempio, i magazzinieri, gli addetti alla produzione, alla manutenzione o alla pulizia sempre che – per particolari esigenze - non effettuino trattamenti di dati personali.

B Formazione specifica

L'impresa deve prevedere una specifica formazione per il personale che svolge determinati trattamenti di dati personali, affinché siano chiare le finalità, i limiti e le modalità dei trattamenti stessi.
Pertanto, l'imprenditore – a seconda delle proprie esigenze organizzative – potrà affiancare alla formazione generica una formazione specifica organizzata in moduli tematici.
La formazione specifica, quindi, **non rappresenta un obbligo generale per tutte le imprese**, bensì è rimessa alla valutazione dell'imprenditore, in base al principio dell'*accountability*.

I principali moduli tematici sono:
Marketing
Videosorveglianza e geolocalizzazione
……
Ulteriori moduli tematici possono essere aggiunti al variare delle esigenze delle imprese e dell'evoluzione normativa e tecnologica.

C Aggiornamento periodico

In coerenza con il principio dell'accountability, spetta all'imprenditore valutare le esigenze formative sulla base della concreta situazione aziendale.

Tra tali esigenze rientra, certamente, quella dell'aggiornamento della formazione del proprio personale dipendente che può risultare necessaria al mutamento delle condizioni aziendali.

L'imprenditore deve, in particolare, prestare attenzione qualora in azienda vengano introdotti nuovi trattamenti di dati personali o nuove tecnologie o intervengano modifiche normative rilevanti.

Alla luce di tali considerazioni, l'aggiornamento sopra indicato non deve essere necessariamente programmato con cadenze fisse (ad es. ogni 5 anni) come accade in altre formazioni fissate obbligatoriamente dalla legge, purché venga effettuato con una certa periodicità.

ADEMPIMENTI NECESSARI PER LA COMPLIANCE: LE MISURE TECNICO - ORGANIZZATIVE

A Misure organizzative

2. Informazione e consenso per clienti e fornitori

L'impresa, nello stesso momento in cui ottiene i dati personali di clienti o fornitori, ha l'obbligo di **fornire le seguenti informazioni all'interessato**:

. il nome dell'impresa che sta trattando i dati (compresi i dati di contatto del responsabile della protezione dei dati, se previsto);
. le finalità per le quali l'impresa utilizzerà i dati;
. le categorie di dati personali interessate;
. la base giuridica per il trattamento dei dati;
. il periodo di tempo durante il quale i dati saranno conservati;
. altre società/organizzazioni/soggetti che riceveranno i dati personali;
. se i dati saranno trasferiti al di fuori dell'UE;

- i diritti di base in materia di protezione dei dati (ad es. il diritto di accesso, di cancellazione, di rettifica, etc.);
- il diritto di sporgere reclamo presso l'autorità per la protezione dei dati personali;
- il diritto di ritirare il consenso in qualsiasi momento, ove presupposto di legittimità del trattamento.

Tali informazioni devono essere presentate in modo conciso, trasparente, intelligibile e redatte in un linguaggio chiaro e semplice. Si parla quindi di **INFORMATIVA**

L'informativa è il documento predisposto dal Titolare in cui vengono spiegati all'interessato tutti gli aspetti relativi al trattamento dei suoi dati personali.

L'informativa deve sempre essere fornita agli interessati per iscritto o con altri mezzi elettronici o oralmente se richiesto dall'interessato, senza necessità di far firmare una ricevuta. E' opportuno pubblicare l'informativa completa sul sito aziendale e farvi riferimento in altri documenti (ad esempio ricevute, contratti, etc.), attraverso una informativa più concisa e semplice.

L'impresa descritta nell'ambito di applicazione delle Linee guida di Confartigianato Imprese non è tenuta ad acquisire il consenso dell'interessato ove il trattamento sia necessario per l'esecuzione del contratto di cui è parte l'interessato o per l'adempimento di un obbligo di legge (GDPR art 6).

Qualora il titolare intenda utilizzare i dati per finalità ulteriori (ad es. marketing) sarà tenuto ad acquisire preventivamente il consenso dell'interessato.

3. Gestione dei dipendenti

L'impresa che abbia uno o più dipendenti è tenuta a contemperare la protezione e la tutela dei dati personali dei lavoratori con gli obblighi e le prerogative del datore di lavoro.

L'impresa deve:

- informare in modo compiuto e chiaro i lavoratori su come tratterà i loro dati, su quali sono le finalità del trattamento e sulle modalità con cui intende raccogliere, trattare e conservare i loro dati;
- acquisire il consenso dei lavoratori in caso di trattamenti che esulano dalla finalità del mero rapporto di lavoro (ad esempio la pubblicazione di foto sui siti o su pubblicazioni. Ad ogni modo, in tale specifica ipotesi è comunque fortemente raccomandato utilizzare modalità di ripresa - ad es. dall'alto o con particolari angolazioni - che non rendano identificabili gli interessati, oppure provvedere ad oscurare - es. con pixellatura - le immagini ove non indispensabili per la finalità perseguita).

In qualità di datore di lavoro, l'impresa deve formare ed aggiornare periodicamente i dipendenti in merito al trattamento dei dati personali.

Inoltre, l'impresa – sulla base della propria attività e tenuto conto della propria organizzazione – deve valutare l'opportunità di:

- autorizzare (per iscritto) i dipendenti al trattamento dei dati personali trattati in azienda;
- fornire istruzioni (possibilmente per iscritto) ai dipendenti sulle modalità consentite di trattamento dei dati aziendali: policy aziendale sull'uso dei dispositivi informatici, delle e-mail (ad es. accesso ai messaggi in caso di assenze prolungate), della navigazione in internet (ad es. download di software o di file musicali, uso di servizi di rete con finalità ludiche o estranee all'attività lavorativa), obblighi derivanti dal GDPR, etc. e le relative sanzioni disciplinari;
- far sottoscrivere apposite dichiarazioni di riservatezza;
- aggiornare le policy dell'Area Risorse Umane (laddove esistente).

4. Nomina dei soggetti che trattano dati all'interno e all'esterno dell'azienda L'impresa è tenuta ad organizzare il trattamento dei dati personali in maniera tale da garantirne la sicurezza anche per quanto riguarda le persone fisiche o giuridiche che entrano in contatto con tali dati (es. attività affidate in outsourcing a soggetti esterni) o sotto la sua responsabilità (es. dipendenti).

La normativa prevede al riguardo due ruoli distinti:

- responsabile del trattamento (GDPR art. 28);
- soggetto autorizzato al trattamento (GDPR art. 29).

4.1. Responsabile del trattamento

Nel caso in cui l'impresa scelga di affidare il trattamento dei dati personali ad un soggetto esterno (esternalizzando ad esempio i servizi di back office, la gestione di applicativi o l'attività di marketing) è tenuto a nominare tale soggetto "Responsabile del trattamento". Il Responsabile del trattamento può essere una persona fisica o una persona giuridica e deve possedere "*garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato*".
Il titolare, pertanto, deve **accuratamente selezionare il responsabile del trattamento** attraverso controlli preventivi, quali ad esempio il possesso di certificazioni riconosciute o autodichiarazioni sulle proprie competenze in materia di protezione dei dati o adesioni a codici di condotta o verifica dell'assenza di eventuali precedenti illeciti nell'ambito del trattamento di dati.

La nomina del Responsabile deve essere formalizzata in un contratto (o altro atto giuridico) in cui siano necessariamente indicati i seguenti elementi:

- le **caratteristiche del trattamento affidato** al responsabile (natura, finalità e durata del trattamento; tipologia di dati trattati e categorie di interessati);

- l'obbligo di trattare i dati soltanto previa **istruzione documentata da parte del titolare** del trattamento

- la garanzia che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- che siano **adottate tutte le misure richieste per la sicurezza** del trattamento;
- che in caso di nomina di un **sub-responsabile del trattamento** sia chiesta un'autorizzazione scritta del titolare e che siano previste, nell'atto di nomina, particolari garanzie per il rispetto del GDPR;
- la previsione, in relazione alla natura del trattamento, che il Responsabile **assista il titolare** con misure e tecniche organizzative, **al fine di soddisfare** l'obbligo di quest'ultimo di soddisfare **le richieste dell'interessato**;
- fornire assistenza al titolare del trattamento nell'ambito degli obblighi che fanno capo al titolare, attinenti alla sicurezza del trattamento (art. 32) ed alla consultazione preventiva (art. 36);
- su richiesta del titolare del trattamento, il Responsabile deve **cancellare o restituire** tutti i dati personali al termine della prestazione dei servizi relativi al trattamento (salvo che il diritto dell'Unione o degli Stati membri non preveda la conservazione dei dati);
- mettere a disposizione del titolare tutte le informazioni necessarie per **dimostrare il rispetto degli obblighi e consentire e contribuire alle attività di revisione, comprese le ispezioni**, realizzate dal titolare del trattamento o da un soggetto da questi incaricato.

4.2 Soggetto autorizzato al trattamento

L'impresa, nella sua qualità di titolare del trattamento, può attribuire a determinati dipendenti funzioni e compiti specifici per il trattamento dei dati.
Si tratta di una facoltà (non di un obbligo) che rientra nell'autonomia organizzativa dell'impresa, ma laddove l'organizzazione aziendale si fa più complessa è opportuno che il titolare attribuisca tali compiti con istruzioni precise.
Non sono previste formalità specifiche, ma è opportuno che il Titolare autorizzi per iscritto i "soggetti autorizzati", individuando, tra l'altro, le istruzioni organizzative e tecniche, il referente, gli obblighi formativi, il vincolo alla riservatezza, i comportamenti da adottare in caso di *data breach*.

Chi sono i soggetti incaricati al trattamento?

- Sono i **dipendenti** dell'azienda
- Devono seguire le istruzioni per il trattamento che sono state fornite dal Titolare
- Devono informare immediatamente il Titolare nel caso in cui vi sia un incidente riguardante il trattamento dei dati
- Devono fornire le informativa agli interessati quando trattano i loro dati
- Devono raccogliere il consenso ed eventualmente le revoche. Per alcuni trattamenti è necessario il consenso dell'interessato (ad esempio per l'invio di materiale pubblicitario a potenziali clienti. Deve comunicare all'interessato che solo una manifestazione espressa della sua volontà, il suo consenso sarà considerato valido. Non sono ammessi consensi impliciti.)
- Devono dare riscontro all'esercizio dei diritti da parte degli interessati

5. Data Protection Officer

Il *data protection officer* (DPO) è una nuova figura introdotta dal GDPR ed è il riferimento per l'azienda per tutto ciò che attiene alla privacy, sia internamente sia nei rapporti con le Autorità di controllo e con gli interessati; è considerato una sorta di *compliance orchestrator*.

L'impresa che opera nei limiti indicati nell'ambito di applicazione delle linee guida di Confartigianato Imprese non ha l'obbligo di nominare il DPO. La designazione del DPO in questi casi è quindi facoltativa.

Per le imprese, infatti, la nomina del DPO è obbligatoria solo in presenza di determinate condizioni (anche se può essere nominato anche su base volontaria), ovvero quando le attività principali dell'impresa consistono in trattamenti su "larga scala":

a) che richiedono il monitoraggio regolare e sistematico degli interessati;
b) di categorie particolari di dati personali o di dati relativi a condanne penali e a reati.

6. Registro dei trattamenti

L'impresa deve tenere il registro dei trattamenti (GDPR art. 30) se effettua trattamenti che:

- possano presentare un rischio (anche non elevato) per i diritti e le libertà degli interessati;
- non siano occasionali;
- o riguardino particolari categorie di dati personali (c.d. 'sensibili') o i dati giudiziari (relativi a condanne penali e a reati).

In tali casi il Garante per la Protezione dei Dati ha precisato che sono tenuti all'obbligo di redazione del registro, ad esempio: esercizi commerciali, esercizi pubblici o artigiani **con almeno un dipendente** (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.).

Ha precisato, inoltre, che l'obbligo di redazione del registro può essere circoscritto alle sole specifiche attività di trattamento sopra individuate (es. ove il trattamento delle categorie particolari di dati si riferisca a quelli inerenti a un solo lavoratore dipendente, il registro potrà essere predisposto e mantenuto esclusivamente con riferimento a tale limitata tipologia di trattamento).

L'impresa nei casi suddetti dovrà tenere il registro dei trattamenti – in forma scritta, anche elettronica, che deve contenere le seguenti informazioni:

a) il nome e i dai di contatto del titolare del trattamento;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati; compresi eventuali responsabili del trattamento dei dati, nonché i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
f) i termini ultimi previsti per la cancellazione elle diverse categorie di dati;
g) una descrizione generale delle misure di sicurezza tecniche e organizzative

ATTENZIONE:
"Documento di censimento e analisi dei trattamenti effettuati dal Titolare o **Responsabile**, in grado di mappare e mantenere aggiornati i trattamenti di dati personali posti in essere all'interno di una organizzazione, nonché indispensabile per ogni attività di valutazione ed analisi del rischio privacy".
Anche il Responsabile del Trattamento deve tenere un proprio Registro delle attività di trattamento

REGISTRO SEMPLIFICATO DELLE ATTIVITA' DI TRATTAMENTO DEL TITOLARE E RESPONSABILE

Modello per le PMI - titolare

SCHEDA REGISTRO DEI TRATTAMENTI *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*							
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*							
RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*							
TIPOLOGIA DI TRATTAMENTO	**FINALITA' E BASI LEGALI DEL TRATTAMENTO**	**CATEGORIE DI INTERSSATI**	**CATEGORIE DI DATI PERSONALI**	**CATEGORIE DI DESTINATARI** *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	**TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI** *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	**TERMINI ULTIMI DI CANCELLAZIONE PREVISTI**	**MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE**

Modello per le PMI - responsabile

SCHEDA REGISTRO DEI TRATTAMENTI DEL RESPONSABILE/SUB-RESPONSABILE *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*		
RESPONSABILE *[inserire la denominazione e i dati di contatto]*		
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*		
RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*		
CATEGORIA DI TRATTAMENTO	**TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI** *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	**MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE**

7. Definizione delle procedure

7.1 Esercizio dei diritti dell'interessato

L'impresa deve predisporre misure idonee per consentire l'esercizio dei seguenti diritti da parte degli interessati (GDPR art. 15 - 22):

. diritto di accesso e di informazione sui trattamenti dei suoi dati personali in corso di esecuzione;

. diritto di rettifica dei dati personali inesatti;

. diritto alla limitazione del trattamento;

. diritto alla cancellazione (oblio) dei dati (se non vincolato da disposizioni legislative sulla durata della conservazione dei documenti aziendali o ove il trattamento non sia giustificato da altra base giuridica quale ad es. il recupero di un credito);

. diritto alla portabilità (solo quando si basa sul consenso espresso o sull'esecuzione di un contratto e viene effettuato mediante mezzi automatizzati;

. diritto di opposizione.

L'impresa deve:

. **informare** l'interessato sulla possibilità di esercitare i suddetti diritti nell'informativa indicando anche i recapiti ove far pervenire la richiesta (indirizzo di posta cartacea o elettronica);

. **monitorare** costantemente la ricezione di eventuali richieste, dando indicazioni ai dipendenti;

. **dotarsi di strumenti** (anche informatici) che le consentano di dare seguito alle richieste di esercizio di un diritto (ad esempio cancellare o modificare un dato personale);

. in caso di richiesta di esercizio di un diritto deve **rispondere all'interessato**, fornendo le informazioni richieste, senza ingiustificato ritardo e, comunque, al più tardi entro **un mese** dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. In tal caso l'impresa deve informare l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

Nell'ipotesi in cui non dovesse ottemperare alla richiesta dell'interessato, l'impresa informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo all'autorità di controllo e di proporre ricorso in sede giurisdizionale.

Le informazioni fornite all'interessato e l'esercizio dei diritti riconosciuti sono gratuiti. Se le richieste sono manifestatamente infondate o eccessive, il titolare del trattamento può:

. addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure

. rifiutare di soddisfare la richiesta.

7.2 Data Breach

Nel caso di una violazione della sicurezza dei dati che comporti - 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, l'impresa senza ritardi e, ove possibile, entro 72 ore dalla scoperta, deve **notificare la violazione al Garante** per la protezione dei dati personali, a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche.

Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

La notifica al Garante va fatta **solo in caso di violazione di dati personali che presenti un rischio per i diritti e le libertà delle persone** come ad esempio in caso di discriminazione, furto d'identità o rischio di frode, perdita finanziaria, danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

La tipologia di trattamenti oggetto delle Linee guida di Confartigianato Imprese rende limitato il rischio che un evento di *data breach* possa arrecare danni agli interessati.

Ad ogni modo, **l'adozione di particolari misure tecniche riduce ulteriormente la necessità che in caso di *data breach* l'impresa sia obbligata ad effettuare la comunicazione al Garante e agli interessati**.

È quindi fondamentale che l'impresa progetti e mantenga un adeguato livello di sicurezza, da configurare in base al proprio livello di rischio - "basso" o "medio" - secondo la classificazione di Confartigianato Imprese.
Sulla base di tale valutazione l'impresa potrà, ad esempio, proteggere con particolari misure (ad esempio la cifratura o la pseudonimizzazione) i dati di maggior rilievo per gli interessati (quali i dati particolari dei dipendenti o dati bancari).
Ad ogni modo, l'impresa deve essere in grado di fornire in caso di controllo le motivazioni in base alle quali – in caso di *data breach* – abbia valutato di non procedere alla notifica al Garante.

Nel caso in cui sia comunque necessario effettuare tale notifica, questa va inviata all'indirizzo: **protocollo@pec.gpdp.it** e deve contenere almeno le seguenti informazioni (art. 33, par. 3 del GDPR):

. una descrizione della natura della violazione dei dati personali, che comprenda, se possibile:

- le categorie e il numero approssimativo di persone interessate;
- le categorie e il volume approssimativo di dati personali interessati;

. il nome e i riferimenti di contatto del responsabile della protezione dei dati (se designato dal titolare) o comunque di un referente competente a fornire informazioni;
. una descrizione delle possibili conseguenze della violazione dei dati personali;
. una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali, comprese, se del caso, le misure adottate per mitigare eventuali effetti negativi;
. solo in caso di notifica effettuata oltre il termine prescritto di 72 ore, una descrizione dei motivi del ritardo.

In ogni caso l'impresa dovrà documentare tutte le violazioni dei dati personali. Esse potranno ad esempio essere indicate nel Registro delle attività di trattamento.

COME INVIARE LA NOTIFICA AL GARANTE?

A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/
(VEDI: Provvedimento del 27 maggio 2021).

Nella stessa pagina è disponibile un modello facsimile, da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante.

Per semplificare gli adempimenti previsti per i titolari del trattamento, il Garante ha ideato e messo disposizione un apposito strumento di autovalutazione (self assessment) che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

B Misure di sicurezza tecniche

L'impresa, al fine garantire un livello di sicurezza adeguato ai rischi del trattamento, deve definire anche un sistema di misure di sicurezza tecniche adeguate al trattamento e all'organizzazione aziendale.
L'impresa deve tenere in considerazione quantomeno i seguenti aspetti della sicurezza.

1)Sicurezza fisica
L'impresa deve ad esempio:
. posizionare estintori vicino ai pc e ai server;
. limitare l'accesso agli archivi cartacei alle sole persone autorizzate;
. assicurarsi che i locali dove sono conservati dati personali siano adeguatamente protetti soprattutto durante l'assenza del personale o la chiusura degli uffici (chiusura con chiavi e sistemi di allarme).

2)Sicurezza dei dati trattati con modalità cartacea
L'impresa deve ad esempio assicurarsi che:

- le persone non autorizzate non possano accedere a documenti contenenti dati personali;
- i documenti con dati personali vengano lasciati incustoditi (ad es. sulle scrivanie);
- i documenti con dati personali vengano conservati in modo sicuro (ad es. armadi chiusi a chiave);
- le fotocopie di documenti contenenti dati personali siano distrutte o rese illeggibili.

B Misure di sicurezza tecniche

3) Sicurezza informatica

L'impresa deve ad esempio:

. assicurarsi che l'accesso ai dispositivi (pc, *smartphone*, *tablet*, etc.) sia protetto da credenziali differenti per ogni utente;

. garantire la sicurezza delle password;

. adottare un'identificazione a più fattori;

. informare/formare i dipendenti sull'uso di internet e della strumentazione elettronica;

. assicurarsi che la rete *wi-fi* sia protetta adeguatamente da password e l'eventuale limite all'accesso da parte di specifici terminali.

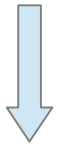
4) Back-up, leggibilità, ripristino

L'impresa deve ad esempio:

- effettuare il back up di tutti i dati (sia su server, sia su client) almeno settimanalmente su supporto esterno (cartuccia/cassetta, NAS, HDD-USB, etc.) in base ad una procedura predefinita;
- effettuare ulteriori back up, ad esempio mensili, semestrali, annuali;
- effettuare prove per il ripristino dei dati su PC/server in tempi certi (al massimo 7 giorni) e compatibili con i diritti dell'interessato.

GESTIONE DEL RISCHIO

RISCHIO ⇨ "Scenario descrittivo di un evento e delle relative conseguenze, che Sono stimate in termini di gravità e probabilità" per i diritti e le Libertà degli interessati" (Linee guida del Gruppo di lavoro Articolo 29 WP)



COME SI GENERA UN RISCHIO?

GESTIONE DEL RISCHIO

MINACCIA

– Accesso abusivo al sistema informatico sia ad opera di hacker che di terzi non autorizzati
- Trasmissione dati in modo non sicuro
- Azione di virus informatici o di programmi suscettibili di recare danno
- Malfunzionamento, indisponibilità, degrado degli strumenti
- Intercettazione di informazione di rete

Che sfrutta una

VULNERABILITA'

– Accessi non autorizzati
- Eventi naturali
- Instabilità dell'alimentazione
- Errori degli utenti o degli operatori

Che genera un

RISCHIO

– Distruzione
- Perdita
- Modifica
- Divulgazione non autorizzata
- Accesso non autorizzato

Che provoca un

IMPATTO SU INTERESSATI

–Ricezione di una comunicazione Indesiderata
- Perdita di riservatezza
- Perdite economiche
- Danno alla salute
- Morte

GESTIONE DEL RISCHIO

Anche in materia di protezione dei dati personali si usano le formule del rischio secondo cui **R= G * P**

Gravità - Probabilità

Es.
1= molto bassa
2= bassa
3= media
4= alta
5= molto alta

G \ P					
	5	10	15	20	25
	4	8	12	16	20
	3	6	9	12	15
	2	4	6	8	10
	1	2	3	4	5

CLASSIFICAZIONE DEL LIVELLO DI RISCHIO E RELATIVI ADEMPIMENTI

Le linee guida di Confartigianato Imprese individuano le caratteristiche dei livelli di rischio considerati - basso e medio - indicando per ciascuno le caratteristiche dell'impresa e gli adempimenti necessari per la *compliance*.
Per i trattamenti che non rientrino nel livello di rischio indicato (ad esempio trattamento di categorie particolari di dati che non siano dei dipendenti, o trattamento per finalità ulteriori) l'impresa dovrà effettuare una specifica valutazione del rischio e predisporre le eventuali ulteriori misure di sicurezza tecnico-organizzative in base al principio dell'*accountability*.

A Livello di rischio basso

Caratteristiche dell'impresa
Impresa senza dipendenti
Trattamento di dati personali "comuni"
Archivio cartaceo e/o utilizzo di strumentazione informatica di basso rischio per i dati personali (database clienti - fornitori, sito internet con funzioni esclusive di "vetrina" ed invio e-mail)

Compliance
Adozione/aggiornamento della modulistica (informative, nomine esterne)
Individuazione delle misure tecniche e organizzative di sicurezza
Il Garante consiglia caldamente anche la tenuta del Registro dei trattamenti

CLASSIFICAZIONE DEL LIVELLO DI RISCHIO E RELATIVI ADEMPIMENTI

B Livello di rischio medio

Caratteristiche dell'impresa
. Micro e piccola impresa
. Con dipendenti
. Trattamento di dati personali "comuni" (rientrano in tale tipologia di rischio i trattamenti di dati, anche particolari, dei dipendenti)
. Utilizzo di strumentazione informatica di maggior rischio per i dati personali (newsletter, e- commerce, rete informatica aziendale, etc.)

Compliance
. Adozione/aggiornamento della modulistica (informative, nomine interne ed esterne)
. Valutazione del rischio
. Tenuta del Registro dei trattamenti
. Individuazione delle misure tecniche e organizzative di sicurezza (con particolare attenzione ai trattamenti dei dati particolari dei dipendenti)
. Definizione delle procedure in caso di data breach

DOCUMENTAZIONE PER DIMOSTRARE LA COMPLIANCE AL GDPR

L'impresa deve in ogni momento essere in grado di dimostrare la *compliance* al GDPR attraverso la produzione dei seguenti documenti:
a)analisi dei trattamenti e delle misure tecniche-organizzative (anche in forma di risposte a checklist)
b)modulistica adottata (informative, nomine interne ed esterne)
c)registro dei trattamenti aggiornato (ove adottato)
d)documentazione relativa al periodico controllo delle misure di sicurezza tecniche e organizzative

Verifica della *compliance*

L'impresa deve programmare una verifica periodica della *compliance* con una cadenza indicata nel Registro dei trattamenti, sulla base del rischio della sua attività.
La verifica andrà ad ogni modo effettuata tempestivamente in occasione di aggiornamenti normativi o modifiche delle attività di trattamento dei dati personali.

FOCUS

1) Marketing diretto

L'impresa che svolge attività di marketing *diretto* può effettuare tale trattamento senza la necessità di acquisire lo specifico consenso dell'interessato, qualora rispetti le condizioni previste dall'art. 130, co. 4, del Codice in materia di protezione dei dati personali - d.lgs. n. 196/03 (sotto riportate).

In tal caso infatti il marketing diretto si basa sul legittimo interesse dell'impresa (di cui deve essere fornita adeguata informazione nell'informativa).

Il Garante ha definito i limiti del marketing diretto e gli strumenti utilizzabili dalle imprese. Secondo l'Autorità, in applicazione del principio del bilanciamento degli interessi, "i titolari del trattamento in ambito privato che hanno venduto un prodotto o prestato un servizio, nel quadro del perseguimento di ordinarie finalità amministrative e contabili, **possono utilizzare senza il consenso i recapiti (oltre che di posta elettronica** come già previsto per legge) **di posta cartacea** forniti dall´interessato, ai fini **dell'invio diretto di proprio materiale pubblicitario o di propria vendita diretta o per il compimento di proprie ricerche di mercato o di comunicazione commerciale**.

FOCUS

- L'attività promozionale deve riguardare beni e servizi del medesimo titolare e analoghi a quelli oggetto della vendita

- **l'interessato**, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le menzionate finalità, sia **informato della possibilità di opporsi in ogni momento al trattamento**, in maniera agevole e gratuitamente, anche mediante l'utilizzo della posta elettronica o del fax o del telefono e di ottenere un immediato riscontro che confermi l'interruzione di tale trattamento;

- **l'interessato medesimo**, così adeguatamente informato già prima dell'instaurazione del rapporto, **non si opponga a tale uso**, inizialmente o in occasione di successive comunicazioni."

2) Sistema di videosorveglianza e strumenti di controllo a distanza dell'attività lavorativa

Con l'espressione **controlli a distanza** si fa riferimento a una particolare tipologia di controlli datoriali, temporali e spaziali, caratterizzati dall'utilizzo di apparecchiature tecnologiche (quali ad es. videosorveglianza e geolocalizzazione).

Nel caso in cui siano presenti sistemi di controllo a distanza l'impresa deve assicurarsi di aver adempiuto agli obblighi previsti dalla normativa di riferimento in materia di lavoro (art. 4 della L. 300/70).

L'impresa deve, quindi, essere autorizzata a tale installazione da accordo sindacale o in assenza di rappresentanze sindacali, dall'Ispettorato territoriale del lavoro competente e dare adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai lavoratori.

FOCUS

In caso di videosorveglianza, oltre all'informativa estesa, l'impresa deve apporre l'informativa breve in modo che sia visibile prima di accedere al luogo videosorvegliato.

Nel caso in cui i sistemi di videosorveglianza e geolocalizzazione siano gestiti da soggetti esterni, l'impresa deve nominare tali soggetti responsabili del trattamento (con contratto o altro atto giuridico), individuando le misure e le garanzie specifiche.

L'impresa deve prestare attenzione al settaggio dei sistemi informatici installati dall'azienda fornitrice dei servizi di videosorveglianza e geolocalizzazione affinchè questi siano adeguati, secondo i principi di privacy by design e by default, alle finalità di trattamento effettivamente perseguite dal Titolare.

METADATI

Il Garante, con Provvedimento del 6 giugno 2024 intende regolamentare l'uso dei servizi informatici di gestione della posta elettronica nel contesto lavorativo, con particolare attenzione ai metadati generati e raccolti dai sistemi di posta elettronica aziendali.

L'obiettivo è garantire che il trattamento dei dati avvenga in modo lecito, evitando:

- Monitoraggio eccessivo dei dipendenti attraverso la raccolta sistematica di informazioni sulle loro attività.

- Conservazione illimitata dei metadati, che potrebbe portare a trattamenti non conformi al GDPR.

- Accessi non controllati ai dati personali, in violazione delle norme di protezione dei dati e dello Statuto dei Lavoratori.

METADATI

Il provvedimento distingue tra:

- **Contenuto delle email** (protetto dal diritto alla riservatezza e alla corrispondenza).
- **Metadati** (informazioni tecniche generate automaticamente dai sistemi di posta, come orari di invio/ricezione, indirizzi IP, destinatari, oggetto del messaggio).

Sebbene i metadati non contengano il contenuto della mail, il Garante evidenzia che possono rivelare informazioni personali sensibili (ad es. con chi un dipendente comunica più spesso, quali clienti o fornitori contatta, la sua frequenza di lavoro, ecc.).

Per questo motivo, il loro trattamento e conservazione devono essere regolati da precise garanzie, evitando il rischio di un controllo indiretto sulle attività dei dipendenti.

METADATI

Le principali indicazioni del Garante Privacy sono:

1. Limitazione della conservazione dei metadati
Il provvedimento stabilisce che la conservazione generalizzata dei metadati per lunghi periodi può essere illecita.
Regola generale: il periodo di conservazione deve essere proporzionato agli scopi perseguiti, con un limite orientativo di 21 giorni. Periodi più lunghi devono essere giustificati con specifiche esigenze aziendali e documentati con una valutazione di impatto (DPIA).

2. Divieto di monitoraggio indiretto dei lavoratori
Il provvedimento chiarisce che l'archiviazione sistematica dei metadati (es. registrare chi scrive a chi, a che ora, con quale frequenza) può costituire controllo a distanza dei dipendenti, violando lo Statuto dei Lavoratori (art. 4, L. 300/1970).
Soluzione: Se l'azienda raccoglie questi dati per finalità organizzative o di sicurezza, deve adottare garanzie adeguate, come l'informativa trasparente ai lavoratori e l'accordo sindacale (se richiesto).

3. Protezione dei dati e responsabilità del datore di lavoro

Il datore di lavoro è responsabile del trattamento dei dati personali derivanti dall'uso della posta elettronica aziendale e deve garantire che:

I fornitori di servizi di posta elettronica adottino misure adeguate alla protezione dei dati.

I lavoratori siano informati in modo chiaro e trasparente sulla raccolta e l'uso dei loro dati.

Le policy aziendali definiscano tempi di conservazione, accessi autorizzati e finalità lecite del trattamento..

METADATI

Premesso che la base giuridica del trattamento dei metadati risiede – come evidenziato dal provvedimento del Garante – nella disciplina giuslavoristica e in particolare negli articoli 4 e 8 della legge 300/70, richiamati espressamente dagli articoli 113 e 114 del Codice della privacy, si forniscono di seguito le seguenti indicazioni in tema di trattamento e conservazione dei metadati.

Conservazione entro i 21 giorni (applicazione dell'articolo 4, comma 2 della legge 300/70)

1) aggiornare l'informativa da rendere al lavoratore, indicando specificatamente trattamento dei metadati e il loro periodo di conservazione;
2) aggiornare il registro dei trattamenti, facendo specifico riferimento al trattamento dei metadati e il loro periodo di conservazione;

Conservazione per un periodo superiore a 21 giorni per assicurare funzionamento e la sicurezza del sistema di posta elettronica (applicazione dell'articolo 4, comma 2 della legge 300/70)

3) quanto indicato nei punti 1 e 2

METADATI

4) redigere un apposito documento dando specifico conto della presenza delle particolari condizioni che richiedono l'estensione del periodo di conservazione oltre i 21 giorni sempre nell'ambito della finalità tesa ad assicurare il funzionamento e la sicurezza delle infrastrutture del sistema di posta elettronica. In particolare occorre indicare:

- le peculiarità che motivano la necessità di conservazione per un periodo superiore ai 21 giorni, ivi compresa l'eventuale impossibilità di impostare una data retention personalizzata, in quanto non consentito dal fornitore. In tal ultimo caso è opportuno allegare la richiesta al proprio responsabile del trattamento/provider di impostare il periodo di conservazione dei metadati in base alle proprie esigenze;
- la data retention individuata che dovrà essere comunque proporzionata;
- una valutazione di impatto con le misure tecnico-organizzative adottate (ad es. per limitare l'accesso ai metadati e tracciarne l'accesso).

METADATI

Conservazione per un periodo superiore a 21 giorni per finalità diverse dal funzionamento del sistema di posta elettronica (applicazione dell'articolo 4, comma 1 della legge 300/70)

5. quando indicato nei punti da 1 a 2

6. oltre agli obblighi giuslavoristici di cui all'art. 4, comma 1, dello Statuto dei lavoratori, valutare se occorre redigere la DPIA, necessaria ad esempio quando i trattamenti riguardano interessati che sono "soggetti vulnerabili" (come nel caso dei lavoratori) e contemporaneamente vengono utilizzati strumenti tecnologici particolari.

Con riferimento, all'eventuale impossibilità di impostare una *data retention* personalizzata, in quanto non consentito dal fornitore, Confartigianato ha sottolineato tale problematica nell'interlocuzione con il Garante che ha preso atto delle difficoltà riscontrate e ha rappresentato che terrà conto del problema, anche alla luce della raccomandazione per i fornitori di servizi – contenuta nel documento di indirizzo – di applicare i principi di protezione dei dati fin dalla progettazione e per impostazione predefinita ai servizi offerti sul mercato.

ACCERTAMENTI ISPETTIVI

I titolari devono fornire collaborazione al Garante della protezione dei dati in caso di accertamenti ispettivi.

Gli accertamenti ispettivi, svolti da personale dell'Autorità e/o dal Nucleo Speciale Privacy della Guardia di finanza, possono essere di natura:

- collaborativa, ai sensi dell'art. 157 del Codice;
- autoritativa, con accessi diretti alle banche dati e agli archivi, ai sensi dell'art. 158 del Codice.

La collaborazione del titolare è elemento di valutazione e di eventuale riconoscimento di circostanze aggravanti o attenuanti nel procedimento per l'applicazione di sanzioni pecuniarie amministrative.

Oltre a ciò, la cooperazione fra titolare e autorità di controllo è espressamente richiesta dall'art.31 del GDPR

Quali sono le EVENTUALI CONSEGUENZE per un'impresa in caso di mancato rispetto della normativa sulla Privacy?

Le **conseguenze di una violazione** delle norme in materia di protezione dei dati personali possono essere:

- Di natura amministrativa (Correttiva e/o Pecuniaria)
- Di natura penale
- Di natura civilistica (ad es. risarcimento del danno)

Le sanzioni amministrative pecuniarie si distinguono nel Regolamento Europeo (UE) 2016/679 in due gruppi:

- Sanzione pecuniaria **fino a 10 milioni di euro o 2% del fatturato mondiale annuo antecedente** (ad esempio per violazioni riguardanti privacy by default – i dati strettamente necessari alle finalità previste e per periodo strettamente necessario -, mancata nomina del responsabile del trattamento, il registro dei trattamenti, la sicurezza, mancata notifica data breach)

- Sanzione pecuniaria **fino a 20 milioni di euro o 4% del fatturato mondiale annuo antecedente** (per violazione obblighi più rigidi del Regolamento o per mancato rispetto obblighi Garante ad es. trattamento illecito dei dati senza una base giuridica valida, violazione dei principi fondamentali del trattamento dei dati art. 5 GDPR)

GRAZIE A TUTTI PER L'ATTENZIONE

Servizio privacy

0547 642511

privacyservizio@confartigianatofc.it

www.confartigianatofc.it