ADEGUAMENTO AL NUOVO REGOLAMENTO PRIVACY

Le risposte alle principali domande delle micro e piccole imprese

Confartigianato Imprese

SOMMARIO

GLI ATTORI DELLA PRIVACY

REGISTRO DEI TRATTAMENTI

TRATTAMENTI AUTOMATIZZATI (PROFILAZIONE)

PRIVACY BY DESIGN E BY DEFAULT

AMBITO DI APPLICAZIONE DEL REGOLAMENTO

Al fine di dare opportuni chiarimenti e offrire un utile strumento operativo alle Associazioni Territoriali ed alle imprese associate a Confartigianato il Gruppo di Lavoro Privacy Confederale ha elaborato il seguente documento che riporta le principali novità della materia riportate nella forma di FAQ.

INFORMATIVA

Che cos'è l'informativa? Quali informazioni devo comunicare alla persona di cui sto raccogliendo i dati?

Al momento della raccolta dei dati, è necessario comunicare chiaramente alle persone di cui si stanno raccogliendo i dati almeno quanto segue (c.d. "informativa"):

- i dati dell'impresa (dati di contatto del titolare ed eventualmente quelli del responsabile della protezione dei dati);
- perché l'impresa utilizzerà i dati personali (finalità);
- le categorie di dati personali interessate;
- la giustificazione giuridica per il trattamento dei dati (base giuridica);
- quanto tempo saranno conservati i dati;
- chi altro potrebbe riceverli (sia altri titolari che responsabili del trattamento);
- se i dati personali saranno trasferiti a un destinatario al di fuori dell'UE;
- i diritti esercitabili dall'interessato;
- il loro diritto di presentare un reclamo presso le autorità competenti per la protezione dei dati personali;
- il loro diritto di revocare il consenso in qualsiasi momento;
- se applicabile, l'esistenza di un processo decisionale automatizzato e la logica implicita, comprese le relative conseguenze.
- Consulta l'elenco completo delle informazioni da fornire **(art. 13 del GDPR)**.

Come devo fornire l'informativa alla persona di cui sto raccogliendo i dati?

L'informativa può essere fornita per iscritto, oralmente su richiesta della persona quando la sua identità è dimostrata con altri mezzi o per via elettronica. L'impresa deve farlo in modo conciso, trasparente, comprensibile e facilmente accessibile, in un linguaggio chiaro e semplice e gratuitamente.
Quando i dati sono ottenuti da un'altra azienda/organizzazione, è necessario fornire alla persona tali informazioni al più tardi entro un mese dal momento in cui si sono ottenuti i dati personali; oppure, nel caso in cui si comunichi con la persona, quando i dati vengono utilizzati per comunicare con lei; oppure, se è prevista la divulgazione a un'altra società, quando i dati personali vengono divulgati per la prima volta.

- L'impresa è inoltre tenuta a comunicare alla persona le categorie di dati e la fonte da cui ha ottenuto i dati; e, nel caso li ha ottenuti da fonti accessibili al pubblico, deve fornire anche

questa informazione. In circostanze specifiche elencate all'articolo 13, paragrafo 4, e all'articolo 14, paragrafo 5, del GDPR, può essere esonerato dall'obbligo di informare la persona **(artt. 13 e 14 del GDPR).**

Posso continuare ad usare i moduli dell'informativa già utilizzati? Quali sono i nuovi contenuti dell'informativa?

L'impresa deve revisionare i moduli dell'informativa attualmente in uso per verificare se vi siano tutti gli elementi previsti dal Regolamento.
In particolare tali moduli vanno integrati con i seguenti nuovi contenuti necessari:

- base giuridica del trattamento;
- periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo;
- esplicito riferimento ai diritti attivabili dagli interessati.
- Vi potranno poi essere alcuni contenuti eventuali che, ove presenti, vanno inseriti nel modulo dell'informativa:
- legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- esistenza di un processo decisionale automatizzato compresa la profilazione con informazioni sulla logica usata, l'importanza e le conseguenze previste per l'interessato;
- eventuale trasferimento dei dati in Paesi extra-UE.

L'impresa deve, inoltre, verificare che l'informativa sia: concisa, trasparente, intelligibile per l'interessato e facilmente accessibile, con un linguaggio chiaro e semplice.

CONSENSO

Quali sono le modalità di acquisizione del consenso al trattamento?

L'impresa deve verificare che, nel caso di trattamenti di dati personali basati sul consenso, quest'ultimo sia stato espresso in modo corretto sia dal punto di vista formale sia da quello sostanziale.

In particolare il consenso deve essere:

- preventivo ed inequivocabile
- informato (preceduto dall'informativa
- specifico (occorre acquisire un consenso per ogni finalità del trattamento, ad esempio il consenso prestato per il marketing indiretto deve essere acquisito separatamente rispetto agli altri eventuali consensi).
- distinguibile da altre eventuali questioni
- revocabile in qualsiasi momento dall'interessato.

Il consenso non può:

- essere tacito o presunto, ma deve essere espresso (il silenzio o l'inattività non equivale al consenso)
- condizionare l'erogazione di un servizio per il quale i dati personali oggetto del consenso non sono necessari.

Se l'impresa tratta categorie particolari di dati (cc.dd. dati sensibili) o effettua decisioni basate su trattamenti automatizzati (ad es. la profilazione) dovrà acquisire dall'interessato un consenso **esplicito**, ovvero prestato separatamente da quello per altri dati personali.
La formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara.

Come deve essere provata l'acquisizione del consenso?

L'impresa deve essere in grado di dimostrare che l'interessato ha prestato inequivocabilmente il consenso a uno specifico trattamento. La forma scritta non è obbligatoria, tuttavia è consigliabile per l'impresa acquisire, ove possibile, il consenso per iscritto oppure, nel caso di servizi on-line, attraverso azioni positive (ad es. "flaggare" una casella o cliccare su un banner). In ogni caso il silenzio o l'inattività non equivale al consenso.

Il consenso ottenuto sulla base del vecchio Codice della privacy è ancora valido?

L'impresa deve revisionare il proprio **modulo** di acquisizione del consenso e adeguarlo alla novità. Per i trattamenti basati sul consenso a norma della precedente disciplina (ovvero tutti i trattamenti sino ad oggi avvenuti) non è necessario che l'impresa acquisisca nuovamente il consenso dell'interessato, se questo è stato espresso secondo modalità conformi al Regolamento. In caso contrario l'impresa deve acquisire nuovamente il consenso.

Come deve essere acquisito il consenso dei minori?

Il consenso dei minori in relazione ai servizi della società dell'informazione è valido a partire dai 16 anni; prima di tale età occorre il consenso dei genitori o di chi ne fa le veci.

CATEGORIE PARTICOLARI DI DATI ("DATI SENSIBILI")

Quali sono le categorie particolari di dati?

Per particolari categorie di dati ("dati sensibili") si intendono:

1. i dati che rivelino:
   - l'origine razziale o etnica
   - le opinioni politiche
   - le convinzioni religiose o filosofiche
   - l'appartenenza sindacale

2. dati genetici (dato che risulta in particolare dall'analisi di un campione biologico della persona fisica)
3. dati biometrici (intesi a identificare in modo univoco una persona fisica, ad esempio le impronte digitali, la conformazione della retina o dell'iride, il timbro e tonalità di voce)
4. dati relativi alla salute (cartelle cliniche, risultati di esami di laboratorio, intolleranze, allergie ecc.)
5. dati relativi alla vita sessuale o all'orientamento sessuale.

In quali condizioni l'impresa può trattare categorie particolari di dati?

Per il trattamento di particolari categorie di dati (dati sensibili) l'impresa deve acquisire il consenso dell'interessato, salvo alcuni casi particolari: ad esempio quando i dati personali sono resi manifestamente pubblici dall'interessato o quando il trattamento sia necessario per:

- assolvere gli obblighi ed esercitare i diritti in materia di diritto del lavoro e della sicurezza sociale e protezione sociale
- esercitare o difendere un diritto in sede giudiziaria
- valutare la capacità lavorativa del dipendente.

Ulteriori condizioni possono essere imposte dalla legislazione nazionale per il trattamento di dati genetici, dati biometrici o relativi alla salute.
Per l'elenco completo delle condizioni per il trattamento dei dati sensibili si veda l'art. 9 del Regolamento **(art. 9 del GDPR).**

Esempio

Non puoi trattare dati sensibili

L'impresa vende abiti online. Per personalizzare i servizi in base agli interessi specifici dei clienti, chiede di fornire informazioni su taglia, colore preferito, metodo di pagamento, nome e indirizzo per la consegna del prodotto. Inoltre, l'azienda chiede al cliente la sua origine etnica. La maggior parte delle informazioni serve per adempiere al contratto, ma l'origine etnica non è necessaria per realizzare e consegnare un abito. Non è pertanto possibile richiederle in base a questo contratto.

CODICE DI CONDOTTA

Che cosa sono i Codici di Condotta e chi può redigerli?

Il Regolamento (Artt. 40-41) prevede la possibilità di elaborare Codici di condotta con la finalità di contribuire alla corretta applicazione della normativa, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

L'elaborazione dei Codici di condotta, è consentita alle Associazioni e agli altri organismi che rappresentano le categorie di titolari del trattamento. Tali organismi possono predisporli, modificarli o prorogarli, allo scopo di precisare l'applicazione del Regolamento.
I Codici di condotta devono essere approvati dal Garante per la privacy.

Quali benefici comporta l'adozione dei Codici di condotta per l'impresa?

L'adozione di Codici di condotta consente di attenuare il rischio connesso al trattamento dei dati personali e contribuisce alla corretta applicazione della normativa sulla "privacy", in funzione delle specificità dei vari settori e delle esigenze specifiche delle micro, piccole e medie imprese. In caso di procedimento da parte dell'Autorità di controllo, l'adesione ai Codici di condotta costituisce, infatti, elemento per dimostrare la corretta applicazione del GDPR ed è uno dei criteri che devono essere tenuti in considerazione per valutare se infliggere una sanzione o per ridurne l'entità.

MISURE DI SICUREZZA E DATA BREACH

Adozione di misure di sicurezza: addio alle misure "minime"?

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" connesso al trattamento. Pertanto dal 25 maggio 2018 non ci saranno obblighi generalizzati di adozione di misure "minime" di sicurezza (previsti dalla precedente disciplina), poiché tale valutazione sarà rimessa, caso per caso, al titolare del trattamento, in rapporto ai rischi specificamente individuati. Tra le possibili misure di sicurezza vi sono la cifratura e la pseudonimizzazione, ovvero modalità di conservazione delle informazioni in una forma che impedisca l'identificazione dell'utente.

Quando può verificarsi il cd. "data breach"?

I dati personali conservati, trasmessi o trattati da un'impresa possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, anche in seguito ad attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. In presenza di violazioni di dati personali (data breach) che possano compromettere le libertà e i diritti dei soggetti interessati, l'impresa deve comunicare la violazione al Garante per la privacy.

Cosa deve fare l'impresa al verificarsi di un "data breach"?

In caso di violazione dei dati personali che comporti un rischio per i diritti e le libertà delle persone fisiche l'impresa DEVE notificare al Garante privacy entro 72 ore da quando ne è venuto a conoscenza. A tale obbligo si aggiunge anche quello di comunicazione agli interessati se il rischio per i diritti e le libertà delle persone fisiche è elevato.

La comunicazione all'interessato non è necessaria se l'impresa ha adottato misure tecnico-organizzative adeguate di protezione (es. la cifratura), o se ha adottato misure che hanno scongiurato il rischio per gli interessati o se la comunicazione richiederebbe sforzi sproporzionati.
In tal senso, aiuterà l'adesione a specifici codici di condotta per attestare e dimostrare l'adeguatezza delle misure tecniche e organizzative di sicurezza adottate dall'impresa.

SANZIONI

Cosa succede se la mia impresa non rispetta le norme sulla protezione dei dati?

Il Regolamento fornisce diverse alternative alle Autorità nazionali (in Italia: l'Autorità Garante per la Protezione dei Dati Personali) in caso di inosservanza delle norme sulla protezione dei dati, a seconda che si sia verificata una:

- possibile violazione: potrà emettere un avvertimento;
- violazione: in questo caso l'Autorità di controllo potrà emettere un ammonimento, un divieto temporaneo o definitivo di trattamento e/o una sanzione pecuniaria fino a 20 milioni di euro, o fino al 4 % del fatturato totale annuo mondiale dell'azienda.

Quali sono i criteri per l'applicazione delle sanzioni?

L'autorità di controllo, nella valutazione sull'applicazione delle sanzioni (che dovranno essere effettive, proporzionate e dissuasive), terrà conto delle circostanze del singolo caso, ossia:

- della natura, gravità e durata della violazione
- del carattere doloso o colposo della violazione
- delle misure adottate per attenuare il danno subito dagli interessati
- delle eventuali precedenti violazioni commesse dal titolare del trattamento
- del grado di cooperazione con l'autorità di controllo
- dell'adesione ai codici di condotta.

La mia impresa può essere ritenuta responsabile per danni?

Gli interessati possono richiedere un risarcimento se un'impresa non ha rispettato il Regolamento sulla protezione dei dati e se hanno subito danni materiali (ad es. perdite finanziarie) o danni non materiali (ad es. perdita di reputazione e stress psicologico).

Quali sono le sanzioni applicabili alle micro e piccole imprese?

Le sanzioni amministrative pecuniarie previste nel Regolamento a seconda della violazione commessa sono le seguenti:

- fino a € 10 milioni, o per le imprese, fino al 2% del fatturato annuo dell'esercizio precedente per inosservanza degli obblighi del titolare e del responsabile del trattamento;

- fino a € 20 milioni, o per le imprese, fino al 4% del fatturato annuo dell'esercizio precedente per: inosservanza dei principi base del trattamento; inosservanza dei diritti degli interessati; inosservanza delle disposizioni sul trasferimento dei dati personali in paesi terzi; inosservanza di un ordine, limitazione provvisoria o definitiva o di un ordine di sospensione dei flussi da parte dell'autorità di controllo:
- fino a € 20 milioni, o per le imprese, fino al 4% del fatturato annuo dell'esercizio precedente per: inosservanza di un ordine correttivo dell'autorità di controllo.

GLI ATTORI DELLA PRIVACY

Chi è il titolare del trattamento?

Il titolare del trattamento è 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.

Il titolare ha l'obbligo di:
- mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento
- adottare politiche interne conformi al Regolamento
- essere in grado di dimostrare che il trattamento è conforme al Regolamento (principio dell'accountability)
- essere in grado di dimostrare di avere adottato misure (organizzative e tecniche) adeguate ed efficaci per la protezione dei dati personali
- adeguarsi alle altre indicazioni di cui all'art. 28.3

Il titolare del trattamento decide autonomamente in ordine alle modalità del trattamento dei dati.
È possibile anche la contitolarità del trattamento: ciò avviene allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento.
In questo caso, determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente Regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato. L'accordo deve disciplinare in maniera esaustiva i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Chi è il responsabile del trattamento?

Il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Il responsabile è designato dal titolare con un contratto o con altro atto giuridico idoneo a vincolare detta figura nei confronti del titolare.
Il suddetto contratto deve necessariamente disciplinare

- la durata, natura e finalità del trattamento
- le categorie dei dati oggetto del trattamento
- le categorie di interessati
- gli obblighi e diritti del titolare
- le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e del Regolamento.

Nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile, è consentita la nomina di sub-responsabili del trattamento da parte di un responsabile per specifiche attività di trattamento. Il responsabile risponde dell'inadempimento dell'eventuale sub-responsabile; esso è esonerato dalla responsabilità solo se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

Chi è il Data Protection Officer (DPO)?

Il responsabile della protezione dei dati personali (anche conosciuto con la dizione in lingua inglese data protection officer – DPO) è una figura prevista dal Regolamento (UE) 2016/679.
Si tratta di un soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo. Coopera con l'Autorità (e proprio per questo, il suo nominativo va comunicato al Garante) e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (artt. 38 e 39 del Regolamento).
Il Data Protection Officer (DPO) ha il compito di analizzare, valutare e disciplinare la gestione del trattamento e della salvaguardia dei dati personali all'interno di un'azienda, secondo le direttive imposte dalle normative vigenti: potrà essere un soggetto interno (dipendente o collaboratore) o esterno (società di consulenza) e dovrà possedere competenze sia in aree giuridiche che informatiche e una ampia conoscenza della normativa. Egli esegue le proprie funzioni in completa indipendenza (senza ricevere alcuna istruzione o imposizione gerarchica) e riferisce sul suo operato direttamente ai vertici aziendali, i quali, per la piena esecuzione dei suoi compiti dovranno fornire risorse adeguate.

Quando è obbligatoria la designazione del Data Protection Officer?

La designazione del DPO è obbligatoria se:

- il trattamento è effettuato da un'autorità pubblica o un organismo pubblico (escluse le autorità giurisdizionali nell'esercizio delle loro funzioni), ovvero
- le attività principali del Titolare e del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessi su larga scala, o

- le attività principali del Titolare e del Responsabile del trattamento consistono in trattamenti su larga scala di categorie particolari di dati personali (ex "dati sensibili": idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, biometrici e i dati giudiziari).

Ricorrendo i suddetti presupposti, sono tenuti alla nomina, a titolo esemplificativo e non esaustivo: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; caf e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento.

REGISTRO DEI TRATTAMENTI

Cos'è il registro dei trattamenti?

Il Regolamento prevede che tutti i titolari e i responsabili di trattamento, eccettuate le imprese con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio **(art. 30 del GDPR)**, devono tenere un registro dei trattamenti – in forma scritta, anche elettronica - che deve contenere le seguenti informazioni:

- il nome e i dati di contatto del titolare del trattamento e del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- una descrizione generale delle misure di sicurezza tecniche e organizzative.

Si tratta di uno strumento fondamentale per disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda ed è indispensabile per a valutazione e l'analisi del rischio.
Deve essere esibito, su richiesta, Garante della Privacy
Anche ove non obbligatoria, la tenuta del registro dei trattamenti è consigliata dal Garante della privacy.

Cosa deve fare l'impresa per redigere il registro dei trattamenti?

Per redigere il Registro dei trattamenti l'impresa deve:
- effettuare una mappatura dei propri trattamenti interni di dati;
- individuare le misure di sicurezza tecniche e organizzative adottate per prevenire il rischio derivante dal trattamento;
- aggiornare periodicamente il registro alla luce dei cambiamenti aziendali.

Il Garante invita tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a dotarsi del Registro al fine di poter più facilmente dimostrare la compliance alla normativa.

Quali benefici può avere un'impresa che elabora il registro dei trattamenti?

La tenuta del registro dei trattamenti potrebbe costituire uno strumento gestionale utile in quanto permette di avere una mappatura completa dei trattamenti effettuati in azienda e di dimostrare la conformità ai principi del Regolamento, primo fra tutti il principio di rendicontazione (accountability).

TRATTAMENTI AUTOMATIZZATI (PROFILAZIONE)

Cosa si intende per profilazione?

La profilazione è una forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi ad una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, il comportamento, etc.
In sintesi, la profilazione si ha in presenza di 3 elementi:
- un trattamento automatizzato;
- eseguito su dati personali;
- con lo scopo di valutare aspetti personali di una persona fisica.

Cosa deve fare un'impresa che decide di ricorrere alla profilazione?

L'impresa deve informare gli interessati dell'esistenza di una decisione basata sul trattamento di dati automatizzato. Nell'**informativa** devono essere chiarite le modalità e le finalità della profilazione. Inoltre, deve essere resa nota la logica inerente il trattamento e le conseguenze previste per l'interessato. A meno che la profilazione non sia necessaria per la conclusione di un contatto o che sia autorizzata dal diritto dell'Unione Europea o di uno Stato membro, il titolare del trattamento deve richiedere il **consenso esplicito dell'interessato**. A meno che non sia diversamente stabilito dall'autorità di controllo, tutte le imprese che svolgono trattamenti automatizzati di dati personali saranno tenute a effettuare la **valutazione d'impatto sulla protezione**

dei dati (DPIA) ed eventualmente a predisporre adeguate misure di sicurezza.

PRIVACY BY DESIGN E BY DEFAULT

Cosa significa protezione dei dati by design (fin dalla progettazione) e by default?

La protezione dei dati personali diventa un elemento essenziale all'interno del processo di organizzazione e pianificazione aziendale. Infatti, il principio di protezione dei dati personali dovrà essere tenuto in considerazione fin dalle prime fasi della progettazione delle attività di trattamento e per tutto il ciclo di vita del dato. Si tratta di costruire un efficiente sistema di protezione dei dati personali che, di default, e senza ostacolare il perseguimento delle finalità del trattamento, consenta di minimizzare la quantità di dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità dei dati stessi.

Cosa deve fare l'impresa per rispettare la 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;
- quando possibile, ricorrere alla pseudonomizzazione (alterazione del dato personale in modo che non possa più essere attribuito a un interessato specifico senza l'utilizzo di informazioni aggiuntive, conservate separatamente);
- ricorrere alla cifratura (codifica dei messaggi in modo che solo i soggetti autorizzati possano leggerli);
- garantire il ripristino dei dati in caso di danneggiamento o malfunzionamento del sistema informativo;
- effettuare una periodica cancellazione dei dati personali non più necessari.

Cosa deve fare l'impresa per rispettare la 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.

Ad esempio: se un'azienda vuole predisporre una banca dati dei propri clienti all'interno della quale sono contenute informazioni di diversa natura, l'accesso alle informazioni andrebbe limitato, in modo che il personale possa visualizzare unicamente le informazioni di cui ha necessità. In secondo luogo, si potrebbe ricorre alla pseudonimizzazione in modo che, solo chi ha il compito di gestire i rapporti diretti con i clienti abbia la possibilità di venire a conoscenza della loro identità. Nel momento in cui il cliente cessa il rapporto commerciale con l'azienda, e comunque venuti a meno qualsiasi obblighi di conservazione dei dati, l'azienda dovrebbe essere in grado di

cancellare (di default, laddove la conservazione non è giustificata da un obbligo di legge) tutti i dati personali riguardanti quel cliente. Infine, sarebbe opportuno impostare un sistema automatico di cifratura dei messaggi nel momento in cui, internamente o esternamente all'azienda, vi è la necessità di trasmettere messaggi contenenti dati personali.

AMBITO DI APPLICAZIONE DEL REGOLAMENTO

Le norme del Regolamento si applicano alle micro e piccole imprese?

Sì perché l'applicazione del Regolamento sulla protezione dei dati non dipende dalle dimensioni dell'impresa, ma dalla natura delle sue attività. Le attività che presentano rischi elevati per i diritti e le libertà delle persone, indipendentemente dal fatto che siano svolte da una piccola impresa o da una società di capitali, determinano l'applicazione di norme più severe.
Tuttavia, alcuni degli obblighi del Regolamento potrebbero non applicarsi a tutte la micro e piccole imprese.
Ad esempio, per le imprese con meno di 250 dipendenti non vi è l'obbligo di tenere un registro delle loro attività di trattamento, a meno che il trattamento dei dati personali non sia un'attività regolare, o costituisca una minaccia per i diritti e le libertà individuali o riguardi dati sensibili o casellari giudiziari. Il gruppo di lavoro che riunisce i garanti europei (WP 29) ha chiarito che è sufficiente anche uno solo dei tre tipi di trattamento per far scattare l'obbligo del registro, ma ha anche affermato che l'obbligo di tenuta del registro vale solo per il trattamento a rischio e non per tutti gli altri trattamenti. Ne deriva che l'esenzione dalla tenuta del registro si applica solo alle imprese senza dipendenti, che non trattano categorie particolari di dati o dati relativi a condanne penali o reati, e che utilizzano per il trattamento dei dati solo supporti cartacei.
Analogamente, le micro e piccole imprese dovranno nominare un responsabile della protezione dei dati soltanto se il trattamento dei dati costituisce la loro attività principale e rappresenta una minaccia specifica per i diritti e le libertà individuali (come il controllo delle persone o il trattamento di dati sensibili o di casellari giudiziari), in particolare quando avviene su larga scala (in base al volume dati, alla durata trattamento, e all'estensione geografica).

Le norme del Regolamento si applicano ai dati relativi a una persona giuridica (società)?

No, il Regolamento si applica solo ai dati personali delle persone fisiche, mentre non si applica ai dati delle società o di altre persone giuridiche.
Tuttavia, **le informazioni relative alle imprese individuali possono costituire dati personali se consentono l'identificazione di una persona fisica.**
Le norme si applicano anche a tutti i dati personali relativi a persone fisiche nel corso di un'attività professionale, quali ad esempio i dipendenti di un'azienda/organizzazione, come gli indirizzi e-mail aziendali del tipo «nome.cognome@azienda.it» o i numeri telefonici aziendali dei dipendenti.

A quali imprese si applica il Regolamento?

Il Regolamento si applica alle imprese, anche micro e piccole, che trattano dati personali di persone fisiche (ad es. clienti, fornitori, dipendenti), mentre non si applica al trattamento dei dati delle persone giuridiche.
Il Regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale.

Quali dati posso trattare e in quali condizioni?

Il tipo e la quantità di dati personali che l'impresa può trattare dipendono dal motivo del trattamento e da ciò che si desidera fare con essi.
Occorre rispettare diverse norme chiave, tra cui:

- i dati personali devono essere trattati in **modo lecito e trasparente**, garantendo l'equità nei confronti delle persone di cui si trattano i dati («liceità, correttezza e trasparenza»);
- occorre avere **finalità specifiche** per il trattamento dei dati che devono essere indicate agli interessati quando si raccolgono i loro dati personali. L'impresa non può raccogliere dati personali per scopi non definiti («limitazione delle finalità»);
- l'impresa può raccogliere e trattare solo i dati personali necessari a tale scopo (**«minimizzazione dei dati»**);
- l'impresa deve assicurarsi che i dati personali siano esatti e aggiornati, tenendo conto delle finalità per le quali vengono trattati, e, in caso contrario, correggerli (**«accuratezza»**);
- l'impresa non può utilizzare i dati personali per altri **scopi non compatibili** con la finalità originaria della raccolta;
- 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 (**«limiti di tempo per la conservazione»**);
- 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 («integrità e riservatezza»).

Posso utilizzare i dati per un'altra finalità?

Sì, ma solo in alcuni casi. Se l'impresa ha raccolto i dati sulla base di un interesse legittimo, di un contratto o di interessi vitali, può usarli per un'altra finalità, ma solo dopo aver verificato che la nuova finalità sia compatibile con quella originaria tenendo conto dei seguenti elementi:

- il legame tra la finalità originaria e la nuova finalità;
- il contesto in cui sono stati raccolti i dati (qual è il rapporto tra l'impresa e la persona?);
- tipo e natura dei dati (ad es. sono sensibili?);

- possibili conseguenze dell'ulteriore trattamento previsto (in che modo inciderà sulla persona?);
- esistenza di salvaguardie adeguate (ad es. cifratura o pseudonimizzazione).

Se l'impresa intende utilizzare i dati per statistiche o per ricerche scientifiche non è necessario eseguire il test di compatibilità.
Se l'impresa ha raccolto i dati in base al consenso o a seguito di un obbligo previsto dalla legge, non è possibile alcun ulteriore trattamento al di fuori dei settori coperti dal consenso originale o dalla disposizione di legge. Un ulteriore trattamento richiede un nuovo consenso o una nuova base giuridica.

Esempi
È possibile un ulteriore trattamento
Un'impresa di installazione di impianti ha un contratto con un cliente per la manutenzione della caldaia. Alla fine del primo anno l'impresa utilizza i dati personali del cliente per verificare se ha i requisiti per un contratto di manutenzione a condizioni migliori, di cui informa il cliente. L'impresa può trattare nuovamente i dati del cliente in quanto le nuove finalità sono compatibili con quelle iniziali.
Non è possibile un ulteriore trattamento
La stessa impresa di installazione di impianti banca vuole condividere i dati del cliente con una impresa che vende caldaie, sulla base dello stesso contratto di manutenzione. Questo trattamento non è consentito senza l'esplicito consenso del cliente, in quanto la finalità non è compatibile con la finalità originaria per la quale i dati sono stati trattati.

Quanti dati posso raccogliere?

I dati personali devono essere trattati solo se non è ragionevolmente possibile effettuare il trattamento in altro modo. Dove possibile, è preferibile utilizzare dati anonimi. Qualora siano necessari, i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario allo scopo («minimizzazione dei dati»). È responsabilità dell'impresa, in qualità di titolare del trattamento, valutare la quantità di dati necessaria e garantire che non vengano raccolti dati irrilevanti.

Esempio
Un'impresa di estetista può chiedere ai clienti il nome, l'indirizzo e il numero di carta di credito dei clienti e potenzialmente anche informazioni su allergie o intolleranza (quindi dati relativi alla salute), ma non le loro opinioni politiche.

Per quanto tempo posso conservare i dati? Devo aggiornarli?

I dati vanno conservati per il più breve tempo possibile. Questo periodo deve naturalmente tenere conto dei motivi per cui i dati devono essere trattati, nonché di eventuali obblighi legali

per la conservazione dei dati per un determinato periodo di tempo (ad esempio, leggi nazionali sul lavoro, fiscali o antifrode che impongono di conservare i dati personali dei dipendenti per un determinato periodo di tempo, durata della garanzia sul prodotto ecc.).
L'impresa deve stabilire limiti di tempo per cancellare o rivedere i dati conservati.
L'azienda deve assicurarsi, inoltre, che i dati in suo possesso siano accurati e aggiornati.

Esempio
Dati conservati troppo a lungo senza aggiornamento
L'impresa effettua un preventivo utilizzando i dati personali del cliente. Se al preventivo non segue la stipulazione di un contratto i dati non potranno essere conservati per un periodo ad esempio di 10 anni perché il periodo di conservazione non sembra proporzionato allo scopo. Diversamente, qualora sussista un obbligo di legge per la conservazione del dato, non si applica la regola sopra esposta ed il titolare deve conservare tali dati fino allo scadere del termine fissato dalla legge.

Gli obblighi sono gli stessi indipendentemente dalla quantità di dati gestiti dalla mia impresa?

Il Regolamento si fonda sull'approccio basato sul rischio, per cui le imprese che trattano dati personali sono incoraggiate ad attuare misure di protezione corrispondenti al livello di rischio delle loro attività di trattamento dei dati. Pertanto, gli obblighi per un'azienda che tratta molti dati sono più onerosi di quelli per un'azienda che tratta pochi dati.
Ad esempio, la probabilità di assumere un responsabile della protezione dei dati per un'azienda che tratta un gran numero di dati è più elevata rispetto a quella di un'azienda che tratta pochi dati. Al tempo stesso svolgono un ruolo importante anche la natura dei dati personali e l'impatto del trattamento previsto. Il trattamento di pochi dati, ma di natura sensibile (ad esempio, i dati relativi alla salute), richiede l'attuazione di misure più rigorose per conformarsi al Regolamento.In tutti i casi, l'impresa dovrà rispettare i principi della protezione dei dati e permettere alle persone di esercitare i loro diritti.

Cosa si intende per dato personale?

I dati personali sono tutte le informazioni relative ad una **persona vivente** identificata o identificabile. Anche le varie informazioni che, raccolte insieme, possono portare all'identificazione di una determinata persona costituiscono i dati personali.
I dati personali sottoposti a de-identificazione, cifratura o **pseudonimizzazione**, ma che possono essere utilizzati per re-identificare una persona, rimangono dati personali e rientrano nell'ambito di applicazione della normativa.
I dati personali che sono stati resi **anonimi**, in modo tale che l'individuo non sia o non sia più identificabile, non sono più considerati dati personali. Perché i dati siano veramente anonimi, l'anonimizzazione deve essere irreversibile.
Il Regolamento protegge i dati personali **a prescindere dalla tecnologia utilizzata per trattare tali dati**. Si dice quindi neutrale sotto il profilo tecnologico e si applica sia al trattamento au-

tomatizzato che a quello manuale. Inoltre, non importa come vengono archiviati i dati: in un sistema informatico, tramite videosorveglianza o su carta; in tutti questi casi, i dati personali sono soggetti agli obblighi di protezione stabiliti nel Regolamento.

Esempio di dati personali:
- nome e cognome;
- indirizzo di casa;
- indirizzo e-mail, come nome.cognome@azienda.com;
- numero della carta d'identità;
- dati sulla posizione (ad es. la funzione di posizionamento su un telefono cellulare)*;
- un indirizzo IP (Internet Protocol);
- un ID cookie*;
- l'identificativo pubblicitario del proprio telefono;
- i dati conservati in un ospedale o da un medico, che possono essere un simbolo che identifica univocamente una persona (pseudonimizzazione)

*In alcuni casi è prevista una normativa settoriale specifica che regola, ad esempio, l'uso dei dati relativi alla posizione o all'uso dei cookie: la direttiva e-privacy (direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 (GU L 201 del 31.7.2002, pag. 37) e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio del 27 ottobre 2004 (GU L 364 del 9.12.2004, pag. 1).

Esempi di dati non considerati personali:
- numero di iscrizione al registro delle imprese di una società;
- dati delle persone giuridiche (ad es. società);
- indirizzo e-mail, come info@azienda.com;
- dati resi anonimi.

Quali sono le novità in tema dei diritti dell'interessato?

Il Regolamento garantisce all'interessato, oltre ai diritti già previsti dalla normativa precedente (accesso, rettifica, cancellazione e opposizione), anche tre diritti nuovi:
- portabilità ovvero il diritto di ottenere i propri dati in formato elettronico di uso comune per poterli trasferire ad altro titolare;
- oblio ovvero l'ampliamento del diritto alla cancellazione dei propri dati personali;
- limitazione ovvero il diritto di consentire temporaneamente la sola conservazione dei dati escludendo altri trattamenti.

L'impresa deve assicurarsi che tutti i diritti siano esplicitati nell'informativa in modo puntuale e deve prevedere specifiche procedure per assicurare il concreto esercizio da parte dell'interessato. Al riguardo è utile avere la mappatura chiara e completa dei trattamenti effettuati in modo tale da poter reperire con facilità i dati e rispondere alle richieste degli interessati nei modi e nei

tempi previsti dal Regolamento. Può facilitare tale compito l'adozione di uno strumento informatico gestionale che consenta il recupero dei dati trattati.

Privacy e gestione dei dipendenti

Quali sono i diritti dei dipendenti?

Nel caso di impresa con dipendenti è da tenere in considerazione il rapporto tra la protezione e la tutela dei dati personali del lavoratore e le prerogative del datore di lavoro.
Tra i diritti del dipendente rafforzati dal Regolamento:

- Diritto di essere informato (il datore di lavoro deve essere trasparente nell'informare il lavoratore su come saranno trattati i suoi dati);
- Diritto di accesso (anche dopo la conclusione del rapporto di lavoro il dipendente ha diritto di accedere al proprio fascicolo);
- Diritto di rettifica delle informazioni errate o non più attuali;
- Diritto all'oblio (il dipendente è legittimato a chiedere al datore di lavoro di cancellare i suoi dati personali ad es. quando a seguito della cessazione del rapporto di lavoro non c'è più l'esigenza di conservarli);
- Diritto di limitare il Trattamento;
- Diritto alla portabilità dei dati (ad es. nel caso di un cambio di lavoro).

Quali gli obblighi del datore di lavoro?

Tra gli obblighi del datore di lavoro per il principio di responsabilizzazione:

- Implementare le misure di sicurezza (tecniche ed operative) idonee a dimostrare di aver posto in essere un trattamento dei Dati del dipendente conforme al regolamento;
- Introdurre (o aggiornare) le policy interne, le istruzioni (ad es. su come usare l'email di lavoro ovvero informative privacy individualizzate) e i mansionari da dare ai dipendenti (che potranno contenere anche, ad es., informativa relativamente alle modalità e finalità di raccolta e conservazione dei dati personali contenuti nelle comunicazioni elettroniche in transito sull'account di posta elettronica aziendale), procedere ad audit interni e formare i dipendenti in materia di privacy;
- Aggiornare le policy dell'Area Risorse Umane (laddove esistente);
- Nominare, quando necessario, il DPO che sarà il punto di contatto e riferimento per tutti i dipendenti in caso di tematiche di privacy;
- Porre in essere una Valutazione di Impatto Privacy se il trattamento che intende effettuare può arrecare danno ai diritti ed alle libertà del lavoratore (ad es. per le attività di selezione ed assunzione di nuovi possibili dipendenti).
- Per quanto riguarda la posta elettronica nella policy aziendale dovrà esservi uno specifico riferimento alla conservazione sui server aziendali di tutte le email scambiate nell'ambito della finalità del rapporto di lavoro e delle finalità e modalità di conservazione, dell'esistenza

di una procedura di cancellazione dell'account dopo l'interruzione del rapporto, il trattamento delle comunicazioni per un periodo che può giungere a 6 mesi, il riferimento ad una procedura di autorizzazione dell'accesso dei Dati conservati nei server aziendali e le relative finalità. Si può consentire al lavoratore di delegare un altro lavoratore in caso di assenze prolungate a leggere i messaggi di posta e ad inoltrare al Titolare del Trattamento quelli ritenuti più rilevanti per l'attività lavorativa. In caso di assenze non programmate il datore di lavoro può incaricare altro personale a gestire la posta del lavoratore avvertendo l'interessato e i destinatari. E' necessario specificare con chiarezza se la navigazione su Internet o la gestione di file nella rete interna autorizzi o meno specifici comportamenti come il download di software o di file musicali o l'uso di servizi di rete con finalità ludiche o estranee all'attività lavorativa. Bisogna anche specificare quali conseguenze di tipo disciplinare il datore di lavoro si riserva di comminare qualora constati che la posta elettronica o la rete interna sono state usate indebitamente. I sistemi di software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet ed al traffico telematico la cui conservazione non sia necessaria.

Il datore di lavoro è tenuto ad 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 dati personali.
I datori di lavoro, in qualità di Titolari del trattamento, devono rivedere le proprie privacy policy interne ai sensi del Regolamento inserendo ad esempio le informazioni relative ai contatti del DPO.

Privacy e marketing

Trattare dati per finalità di marketing diretto (forme di pubblicità per il quale un Titolare invia comunicazioni direttamente a uno o più utenti identificati e identificabili per mezzo di servizi di comunicazione elettronica – email, telefono, sms, mms, messaggistica istantanea) può essere considerato "legittimo interesse". L'interessato si può opporre in qualsiasi momento e gratuitamente. Nelle Informative la possibilità di opporsi a tale Trattamento deve essere presentata chiaramente e separatamente da qualsiasi altra informazione.
N.B. per svolgere una campagna di marketing che sia compliant al GDPR, oltre alla disciplina del Regolamento, bisogna tener conto della direttiva 2002/58/CE del 12 luglio 2002 – Direttiva e-Privacy – in corso di revisione in sede parlamentare UE
Per quello che riguarda l'email marketing è importante che il Titolare abbia il consenso dell'interessato prima di inviare un'email a fini di marketing diretto per evitare l'intrusione nella vita privata. E' consentito l'uso dei recapiti e-mail nell'ambito di una relazione commerciale esistente, finalizzato alla proposta di prodotti o servizi analoghi mediante marketing diretto. In ogni caso il titolare deve sempre lasciare la facoltà di revocare agevolmente il consenso in qualsiasi momento e con qualsiasi modalità. Ad es. si potrebbe inserire nell'email un collegamento o un indirizzo di posta elettronica valido cui gli interessati possono inviare la comunicazione con cui revocare il Consenso.

NOTA METODOLOGICA

Il presente Vademecum è stato redatto tenendo conto dei seguenti atti normativi:

Regolamento UE 27/04/2016 n. 679
Il Regolamento, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, è entrato in vigore a maggio 2016 (G.U. U.E. 04/05/2016 n. L119). Dal 25/05/2018 sarà pienamente e direttamente applicato in tutti gli Stati membri dell'Unione.

Legge di Bilancio 2018 (l. 205/17) - articolo 1, commi da 1020 a 1025 che attribuiscono alcuni compiti al Garante della protezione dei dati personali, ai fini dell'adeguamento dell'ordinamento nazionale al Regolamento UE 2016/679:

- si prevede che il Garante debba, entro 2 mesi, adottare un provvedimento per disciplinare: 1) le modalità di monitoraggio e vigilanza sull'applicazione del Regolamento UE; 2) le modalità di verifica che i titolari dei dati personali trattati per via automatizzata o tramite tecnologie digitali siano dotati di infrastrutture adeguate; 3) la predisposizione di un modello di informativa per i titolari di dati personali che effettuano un trattamento con uso di tecnologie digitali fondato sull'interesse legittimo; 4) le linee-guida da applicare quando il trattamento dei dati personali sia fondato sull'interesse legittimo del titolare (comma 1021);
- si prevede che chi intende effettuare un trattamento dati fondato sull'interesse legittimo che prevede l'uso di nuove tecnologie o di strumenti automatizzati, debba preventivamente inviare al Garante l'informativa (redatta in base al modello previsto dal Garante stesso). In assenza di intervento del Garante, trascorsi 15 giorni dalla comunicazione, il trattamento potrà essere avviato (comma 1022). Se invece il Garante ritiene che dal trattamento possa derivare un rischio per gli interessati, dispone una moratoria del trattamento stesso per un periodo massimo di 30 giorni. Se a seguito dell'approfondimento risulta un rischio effettivo il Garante potrà inibire l'utilizzo dei dati personali (comma 1023);
- si prevede che il Garante da conto dell'attività relativa all' applicazione del Regolamento UE nella relazione annuale al Parlamento (comma 1024).

Legge europea 2017 (L. n. 167/2017)
L'articolo 28 della Legge europea ha novellato l'articolo 29 del Codice in materia di protezione di dati personali, prevedendo che il titolare del trattamento dei dati (anche sensibili) possa avvalersi, quale responsabile del trattamento, di soggetti pubblici o privati. In tal caso deve essere stipulato un atto giuridico di nomina in forma scritta, adottato in conformità a schemi-tipo predisposti dal Garante.

Legge di delegazione europea (L. n. 163/17)
L'art. 13 della Legge di delegazione europea ha attribuito al Governo la delega per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) n. 2016/679, da attuare entro sei mesi dalla sua approvazione (quindi entro il 25/05/2018) mediante decreti legislativi, nel rispetto dei seguenti principi e i criteri direttivi:

- abrogazione delle norme del D.Lgs. n. 196/2003 in contrasto o incompatibili con la nuova disciplina europea;
- modifica delle norme del Codice Privacy per la puntuale attuazione alle disposizioni del Regolamento UE;
- coordinamento delle disposizioni vigenti del Codice Privacy con i principi introdotti dal Regolamento;
- possibilità di delega al Garante Privacy per l'adozione di provvedimenti attuativi e integrativi diretti al perseguimento delle finalità previste dal Regolamento;
- adeguamento dell'attuale regime sanzionatorio, a livello penale e amministrativo, alle disposizioni del Regolamento, per garantire la corretta osservanza della nuova normativa.

Pertanto, nei prossimi mesi, si renderà necessario un intervento del Governo per adeguare l'ordinamento interno alla normativa comunitaria che altrimenti vedrà l'applicazione diretta e immediata del Regolamento UE n. 679 a decorrere dal 25/05/2018.

In presente Vademecum non tiene, invece, conto del **Decreto Legislativo 30/06/2003 n. 196**, che ha introdotto nel nostro ordinamento il "Codice per la protezione dei dati personali", in vigore dal 1/01/2004, in attuazione di una direttiva comunitaria del 2003 e abrogativo della precedente Legge n. 675/1996. Tale provvedimento, seppur al momento vigente, a partire dal 25 maggio 2018 dovrà essere disapplicato per le parti confliggenti con il Regolamento europeo.

Alcune risposte sono state elaborate sulla base delle informazioni fornite dalla Commissione Europea sul sito https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_it e dal Garante italiano per la protezione dei dati personali sul sito www.garanteprivacy.it/.