KRUZER

PRIVACY - CYBER SECURITY

La Privacy e la Protezione dei dati personali nelle imprese del settore agricolo

Kruzer, società specializzata in tema di privacy e protezione dei dati personali, ha deciso di mettere a disposizione delle imprese del settore agricolo il presente manuale con l'obiettivo di supportare chi ancora dovesse mettersi in regola con gli adempimenti previsti dalle disposizioni del regolamento europeo 679/2016 (Gdpr) e del successivo d.lgs. 101/2018.

Il manuale fornisce una panoramica sui principali aspetti da considerare in tema di privacy ma non si sostituisce all'intervento di personale esperto, sicuramente necessario almeno nelle realtà più complesse.

Indice

Introduzione

GDPR: General Data Protection Regulation, ovvero Regolamento Generale per la Protezione dei Dati.

Questo acronimo è diventato estremamente diffuso e familiare a seguito della sua applicazione dopo il 26 maggio 2018.
A contribuire alla sua popolarità, alcuni interventi sanzionatori dei Garanti della Privacy europei ed una nuova presa di coscienza sull'importanza della tutela dei propri dati personali, nell'era di Google,Facebook e dei grandi players internazionali del Web.

Il tema della privacy e della protezione dei dati personali, spesso viene riferito ai clienti di un'organizzazione, ma, in realtà coinvolge un numero ben più vasto di soggetti; basti pensare ai dipendenti di un'azienda, ai fornitori, ai consulenti, ai visitatori e, se presente un impianto di videosorveglianza, anche ai semplici passanti, corrieri, addetti esterni alla manutenzione, etc.

Gli organi di stato preposti alla verifica sono rappresentati, in primis, dal **Nucleo Privacy della Guardia di Finanza**, ma non è raro che le verifiche possano essere condotte dai dipartimenti locali, sempre della Guardia di Finanza, ma anche da altri enti, come la **Polizia Amministrativa, l'Ispettorato del Lavoro**, etc. In ogni caso, segnalazioni al Garante della Privacy possono essere inoltrate da qualsiasi cittadino.

Il Regolamento Generale per la Protezione dei Dati è stato realizzato per tutelare i soggetti appartenenti all'Unione Europea, anche quando i loro dati vengono trattati da entità extra-Ue.

Il GDPR non si riferisce solamente ai trattamenti effettuati tramite dispositivi informatici, anche se questi ultimi rappresentano i mezzi più diffusi per raccogliere, conservare ed elaborare dati personali. Infatti, anche un trattamento effettuato tramite documenti cartacei o addirittura oralmente, può essere soggetto a particolari regole e accorgimenti da adottare, secondo i principi generali del Regolamento europeo.

La normativa richiede che qualsiasi soggetto pubblico o privato, che opera come soggetto economico, anche senza scopo di lucro, sia conforme ai principi della normativa e agli adempimenti richiesti, a prescindere dal fatturato, dal numero di addetti che lo compone e dall'attività svolta.
Non sono quindi escluse attività dedicate al commercio al dettaglio; alle manutenzioni; alle attività produttive e di servizi; professionisti; associazioni; cooperative; etc., oltre agli enti della Pubblica Amministrazione.
Di conseguenza, anche le imprese del mondo agricolo, quindi allevatori, agricoltori, venditori all'ingrosso e al dettaglio, terzisti, agenti e aziende di fornitura di prodotti e di servizi del settore, sono chiamate ad adempiere al regolamento europeo, al decreto italiano e alle linee guida espresse dal Garante della Privacy.

Per essere conformi alla normativa, le imprese devono espletare una serie di adempimenti; effettuare la formazione periodica obbligatoria e mantenere un aggiornamento nel corso del tempo tramite interventi di audit e di formazione.

Stampato in Italia

1 - Il Regolamento europeo: cos’è e come essere conformi

Nei prossimi paragrafi, andremo a descrivere le caratteristiche essenziali del regolamento e, utilizzando uno stile molto schematico che dà più spazio alla pratica da svolgere piuttosto che alla pura teoria, elencheremo le principali azioni da compiere per adeguare la propria organizzazione secondo la normativa vigente, fornendo schemi, descrizioni ed esempi.

1- a In cosa consiste la normativa sulla privacy

1) un regolamento europeo (Gdpr) imposto agli stati membri;
2) un insieme di 99 articoli di legge e di 176 «considerando»;
3) un insieme di: provvedimenti; linee guida; modifica codici deontologici;
4) in Italia, il decreto legislativo 101/2018, che ha modificato il nostro codice privacy secondo i principi del Gdpr.

Glossario sintetico:

1) Titolare dei trattamenti dei dati:
   persona o entità che definisce i dati e le finalità dei trattamenti dei dati personali;
2) Responsabile dei trattamenti:
   persona o entità (normalmente esterna alla struttura del Titolare dei trattamenti) che tratta i dati per conto del Titolare dei trattamenti;
3) Autorizzato ai trattamenti: soggetto, generalmente interno all'azienda, autorizzato dal titolare dei trattamenti a trattare i dati personali per suo conto;
4) Base giuridica: fondamento che rende lecito il trattamento dei dati. Per es., il consenso, una legge nazionale, l'esecuzione del contratto, etc.

I fondamenti del Regolamento:

1) Il Regolamento si riferisce ai dati personali, sia particolari (sensibili) che comuni, riferiti ai cittadini, quindi persone fisiche, europei e deve essere applicato da tutte le entità pubbliche e private (aziende e professionisti);
2) Non riguarda i trattamenti di dati effettuati da persone fisiche a scopo privato, tranne che in situazioni molto particolari;
3) Aumenta i diritti dei soggetti interessati (persone alle quali i dati appartengono);
4) Definisce quando e come sia lecito trattare i dati personali;
5) Impone la tutela e la protezione dei dati personali a chi li tratta (titolare del trattamento), che diventa l'unico vero responsabile degli stessi. Egli deve implementare tutte le misure tecniche e organizzative (processi; sicurezza fisica e informatica; policy aziendali; formazione; etc.);
6) Il titolare dei trattamenti deve utilizzare il minimo possibile dei dati ed effettuare solo i trattamenti necessari, limitando, per esempio, la diffusione (anche nei paesi extra Ue) e la conservazione degli stessi;
7) Il titolare dei trattamenti deve trattare i dati utilizzando le basi giuridiche previste (consenso esplicito; normativa nazionale; legittimo interesse; esecuzione del contratto);
8) Il titolare dei trattamenti deve informare sui trattamenti di dati che esegue e deve consentire ai soggetti interessati di esercitare i propri diritti (aumentati rispetto a prima);
9) Il titolare dei trattamenti deve progettare i nuovi processi aziendali, oltre a quelli già esistenti, tenendo conto della "minimizzazione e della sicurezza del trattamento" (privacy by design) e stabilendo un'impostazione di base per l'utilizzo dei dati per la sola finalità prevista (privacy by default) ;
10) Al verificarsi di una violazione di dati (data breach) è previsto un iter specifico, compresa una notifica all'ufficio dell'Autorità del Garante;
11) L'implementazione di alcune tecnologie o processi, definiti a rischio e/o che prevedono trattamenti automatizzati, richiedono la redazione di una valutazione di impatto privacy (Dpia);
12) Le attività che prevedono il trattamento massivo di dati e tutti gli enti pubblici richiedono la presenza del Responsabile della Protezione dei Dati (Dpo), un esperto della materia, super partes in grado di seguire l'azienda o l'ente, nel tempo, al fine di garantire la conformità della struttura al regolamento; la sicurezza dei processi; effettuare la formazione; le valutazioni di impatto e l'eventuale contatto con il Garante e con i soggetti interessati.
13) E' prevista una documentazione specifica, da produrre, a carico dei titolari e dei responsabili dei trattamenti.

L’importanza di essere adeguati si riscontra anche nella formazione obbligatoria per chi tratta i dati personali (art. 29 del Gdpr): circondarsi di un team di collaboratori formati e consapevoli, rispetto ai principali temi riguardanti la sicurezza informatica, la prevenzione delle violazioni e i principi generali di protezione, la tutela e la gestione dei dati personali, significa assicurare la propria organizzazione contro le esiziali conseguenze, sul business e sulla reputazione dell’impresa, causati da fenomeni di phishing, hackeraggio e gestioni illecite del proprio database.

In caso di ispezione, bisogna essere in grado di dimostrare di conoscere i principi fondamentali che regolano il trattamento di dati personali, le misure tecniche e organizzative implementate per la protezione dei dati e la redazione della documentazione prevista dal regolamento.

1- b Sanzioni e risarcimenti

L’art. 83 del GDPR definisce il sistema sanzionatorio applicabile dai Garanti europei, in caso di inadempienze. In realtà, l’operato dei Garanti, in tema di sanzioni, è caratterizzato da un ampio arbitrio ed il regolamento pone esclusivamente dei limiti massimi, definiti in dieci milioni di euro per alcune tipologie di inadempienze e in venti milioni di euro per le inadempienze più gravi. La sanzione può anche essere calcolata sul fatturato dell’azienda se, in quest’ultimo caso risultasse più elevata dei limiti sopraesposti, limitandola al 2% o al 4% del giro di affari mondiale dell’impresa.
Facciamo l’esempio della sanzione comminata a Google in Francia: è stata di cinquanta milioni di euro, quindi calcolata sul fatturato.
Parecchie sanzioni sono state comminate anche a piccole e medie società, ricordiamo un mobilificio, una compagnia di radiotaxi, società dell’area informatica e del marketing e perfino bar, hotel e amministratori di condominio, oltre che ospedali e vari enti pubblici.

Tuttavia, la sanzione non è l’unico strumento del Garante, che, nei casi meno gravi, può agire con semplici “richiami” o con dei divieti temporanei al trattamento di alcune categorie di dati.
Vige la regola dell’”inversione dell’onere della prova”, cioè è il soggetto ritenuto colpevole che deve provare la sua innocenza (o la sua conformità al regolamento).
L’esborso economico di chi viene trovato inadempiente potrebbe non limitarsi alla sanzione se il suo operato o la mancata applicazione delle misure idonee, ha generato un danno a terzi, magari causato da una violazione dei sistemi da parte di malintenzionati. Per esempio, se non vengono applicate idonee misure di sicurezza ai server aziendali e un criminale informatico riesce a mettere in atto una truffa o un furto di identità, il malcapitato può chiedere il risarcimento al titolare o al responsabile del trattamento.

1- c I Dati Personali

Molto spesso si confonde il concetto di dato personale con quello di dato sensibile, tanto che molti imprenditori pensano di non dover effettuare alcun adeguamento, affermando di non trattare questo genere di dato.

Il regolamento europeo è stato adottato al fine di tutelare i diritti e le libertà fondamentali della persona, quindi, si riferisce ai dati riguardanti le persone fisiche, sia quelli sensibili (definiti “particolari” dal nuovo regolamento europeo), cioè i dati relativi alla situazione economica, al credo religioso, alle idee politiche, alla salute, etc., sia i dati di contatto pubblici e non pubblici (es,: il numero dello smartphone; la mail privata; etc.) e tutti quei dati che, trattati singolarmente (es.: le immagini) o abbinati ad altri, inequivocabilmente, identificano una persona fisica.

Quindi, possiamo affermare che tutti gli imprenditori trattano dati personali, spesso anche particolari (pensiamo ai dati appartenenti ai dipendenti e collaboratori), e poco importa che siano dati di clienti, piuttosto che di dipendenti, di collaboratori esterni o di fornitori.

Non rientrano nella considerazione del Gdpr i dati di entità giuridiche, cioè riferibili a società o enti. Per cui, un bilancio, il nome di un amministratore di società, una previsione di fatturato o anche una formula segreta di un’azienda, non sono soggetti al regolamento europeo, ma oggetto di altri eventuali negozi contrattuali o accordi di riservatezza.

Per ricapitolare la definizione dei dati personali, riportiamo una parte di testo presente sul sito del Garante della privacy (www.garanteprivacy.it):

“Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc.

1- d La normativa sulla privacy e l’impresa agricola

Le imprese del settore agricolo possono assumere forme molto diverse, pensiamo, ad esempio, ad un agricoltore ditta individuale con 2 collaboratori e ad una azienda di mangimi con 150 dipendenti. Parliamo certamente di due realtà molto differenti, in termini di organizzazione, di struttura e di dimensioni, eppure alcuni concetti relativi al tema della privacy e della protezione dei dati sono abbastanza simili.

Infatti, entrambe le imprese potrebbero, potenzialmente, gestire:

dati di clienti (entità giuridiche e persone fisiche/ditte individuali) **dati di collaboratori** (persone fisiche); **dati di fornitori** (entità giuridiche e persone fisiche/ditte individuali); **dati di visitatori** (entità giuridiche e persone fisiche/ditte individuali); **sito web** (normative relative i visitatori del sito); rapporti con **imprese esterne** che gestiscono dati di cui hanno la titolarità del trattamento (consulente del lavoro,

commercialista, società di medicina del lavoro, etc.); **smartphone contenente contatti** e mail di lavoro; **pc/server contenenti dati** personali; impianto di **videosorveglianza.**

Da qui è evidente che qualsiasi tipologia di impresa gestisce, anche se in diversa quantità e modalità, dati di persone fisiche e, per questo, è chiamata a rispondere, in caso di violazioni e controversie, davanti al Garante della Privacy e, in generale, in sede civile o penale, anche con risarcimento di eventuali danni a terzi.

Generalmente un’impresa che opera nel settore agricolo può connotarsi tra le seguenti tipologie di azienda, suddivise per macroarea:

- azienda di produzione;

- azienda di produzione e distribuzione al cliente finale;

- azienda di distribuzione (grossista o negoziante);

- azienda di trasformazione;

- agenzia - rappresentanza commerciale;

- azienda agroturistica;

- associazione - consorzio;

- azienda di consulenza e di servizi per il settore.

Le peculiarità di ogni tipologia di impresa sostanzialmente si riferiscono al ruolo dei collaboratori, cioè, chi tratta dati personali e chi no. Spesso una prima distinzione è tra chi svolge mansioni amministrativo/commerciali e chi svolge lavoro manuale, anche se non è detto che questi ultimi non trattino dati (pensiamo ad un operaio, capo squadra, che gestisce i numeri di cellulare dei colleghi; le programmazioni dei loro turni; etc.), alle attività di marketing, in particolare di chi vende direttamente al privato; chi tratta dati sensibili, ad esempio, dati di natura economica e personali (pensiamo ad esempio, a chi vende trattori a rate tramite una finanziaria o chi si occupa di bandi di finanza agevolata per l'agricoltura); a chi gestisce vendite tramite e-commerce.

1- e Gli adempimenti generali e i 10 steps per adeguarsi

Di seguito, verranno elencate “passo passo” (step) tutte le attività da effettuare per adeguare l’azienda alla normativa. Alcune imprese molto piccole, magari a carattere familiare, non si riconosceranno in alcuni modelli proposti. Ogni imprenditore dovrà “plasmare” gli adempimenti della normativa in base alla sua organizzazione e dimensione. Essendoci, nel settore agrario, anche imprese più grandi, abbiamo preferito fornire esempi più completi. Sappiamo bene che in molti casi, ad esempio, non ci sarà l’ufficio del personale o il direttore generale, in quanto nelle micro imprese tali ruoli sono rivestiti direttamente dai titolari. Tuttavia, il titolare è comunque una persona che tratta quei dati, anche con il pc e che li conserva in un ufficio. Ciò, naturalmente, non lo esime ad applicare le pratiche indicate dalla normativa.

Step 1. Identificare tutti gli “strumenti” di trattamento dei dati

La prima operazione da fare, sarà redigere un elenco di tutti i dispositivi che trattano i dati personali, descrivendo le caratteristiche più importanti e i contenuti, come esemplificato nelle tabelle sottostanti. Ricordiamo che, come riportato nel glossario del manuale, il termine “trattamento” comprende qualsiasi operazione effettuata sui dati, come la raccolta, la conservazione, la cancellazione, il confronto, etc.

Tab. 1
ASSET FISICI

Tipo	**Localizzazione**	**Contenuto**	**Caratteristiche**	**Utilizzatori**
Armadio 1	Ufficio direzionale	Dati di clienti: contratti; moduli garanzia.	Chiudibile a chiave	Resp Commerciale
Armadio 2	Ufficio personale	Dati dei dipendenti: timbrature; cud; buste paga; dati di contatto.	In stanza accessibile solo ad autorizzati	Resp. Del personale
Schedario 1	Segreteria	Dati dei visitatori: nome, cognome, ditta, data della visita e orario.	In cassetto chiuso a chiave	Receptionist
Armadio 3	Negozio	Dati di clienti	Chiudibile a chiave	commesso

Tab. 2
ASSET INFORMATICI E TECNOLOGICI

Tipo	**Localizzazione**	**Contenuto**	**Caratteristiche**	**Utilizzatori**
Pc 1	Ufficio direzionale	Dati di clienti: acquisti; fatture; dati di contatto	Windows 10; in rete; antivirus; password	Resp Commerciale
Server 2	Ufficio personale	Dati dei dipendenti: timbrature; ferie; dati per elaborazione paghe	Windows 2012; rete separata; firewall; password;..	Resp. Del personale e impiegato designato
Telecamera 1	Segreteria	Immagini dei visitatori e dipendenti	Senza registrazione; monitor non rivolto verso il pubblico	Receptionist – titolare - impiegato
……	…..	……	……	……

Nell'elenco degli asset tecnologici sono da inserire anche tablet, smartphone, dispositivi di controllo di accesso dei dipendenti, sistemi di cloud e tutte le strumentazioni aziendali che trattano dati personali e devono essere aggiornati periodicamente e riportare gli asset che nel frattempo sono stati aggiunti, eliminati o modificati.
Queste due tabelle evidenziano subito lo stato di sicurezza dei dispositivi, le caratteristiche principali, chi li può utilizzare e che controllo si riesce ad esercitare rispetto al loro utilizzo.

Step 2. Redigere un elenco di tutti i soggetti interni ed esterni alla propria organizzazione che trattano dati personali ed il loro ruolo.

Lo scopo di questo elenco è quello di predisporre un organigramma privacy propedeutico all'attività di nomina in base ai ruoli ricoperti dai soggetti coinvolti nell'attività aziendale. Consigliamo di compilare la colonna "tipo di nomina prevista" solo dopo aver letto il paragrafo successivo, nel quale vengono specificati i criteri da seguire per le nomine e dove vengono spiegati tutti i ruoli dei soggetti coinvolti.

Tab 3
SOGGETTI INTERNI ALL'IMPRESA
Si tratta dei collaboratori di qualsiasi livello gerarchico che trattano qualsiasi tipo di dato personale, a scopo lavorativo, all'interno dell'organizzazione.

Ruolo	**Nome Cognome**	**Trattamenti di dati effettuati (quali dati di quali soggetti)**	**Tipo di nomina prevista**
Direttore Generale	Mario Rossi Cod fiscale:xxxxxx	Dipendenti: tutti i dati; Clienti direzionali: dati di contatto e contratti; fornitori principali: dati di contatto…	Autorizzato ai trattamenti
Responsabile commerciale	Giovanni Bianchi Cod fiscale:xxxxxx	Agenti: dati di contatto; documenti contabili; clienti: dati di contatto e contratti;	Autorizzato ai trattamenti
Impiegato amministrativo	Lorenza Verdi Cod fiscale:xxxxxx	Clienti: dati di contatto e dati fiscali; agenti: dati contabili e fiscali; dipendenti: note spese	Autorizzato ai trattamenti
Responsabile del personale	Giovanna Viola Cod fiscale:xxxxxx	Dipendenti: timbrature; cud e buste paga; dati di contatto; candidati: curriculum vitae	Autorizzato ai trattamenti

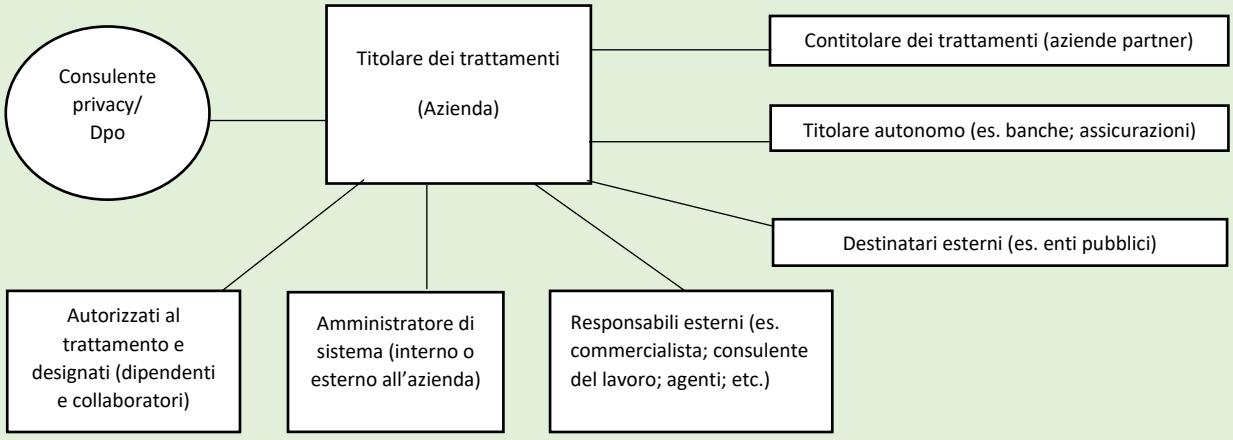
Tab 4
SOGGETTI ESTERNI ALL'IMPRESA
Sono, generalmente, alcuni fornitori di servizi, che, per la natura della propria attività, trattano dati personali la cui titolarità del trattamento originaria è dell'entità di cui stiamo effettuando l'adeguamento.

Ruolo	**Nome Cognome (se professionista o ditta individuale) o Ragione sociale**	**Trattamenti di dati effettuati (quali dati di quali soggetti)**	**Tipo di nomina prevista**
Consulente del lavoro	Mario Rossi Via … num…città…. P.i. ……	Dipendenti: tutti i dati relativi a paghe,	Responsabile esterno

		contributi, timbrature, ferie, etc.;	
Medico competente	Giovanni Bianchi Via … num…città…. P.i. ……	Dipendenti: dati sanitari	Titolare autonomo dei dati
Commercialista	Studio Gamma S.r.l. Via … num…città…. P.i. ……	Clienti: dati fiscali; agenti: dati contabili e fiscali;	Responsabile esterno
Assistenza informatica	Mega Byte S.n.c. Via … num…città…. P.i. ……	Dipendenti: timbrature; cud e buste paga; dati di contatto; candidati: curriculum vitae	Responsabile esterno

Tra i soggetti da considerare "esterni" non vanno dimenticati gli agenti di commercio. Questi soggetti, in base ad alcune peculiarità relative al loro modus operandi e al contratto che norma la loro attività con l'impresa, possono essere considerati "responsabili esterni" se operano con ampia autonomia e con una loro organizzazione definita, al contrario, potrebbero essere considerati "autorizzati ai trattamenti" se monomandatari e se utilizzano gli strumenti forniti dalla mandante, come gli uffici, il tablet, il gestionale, etc.

Step 3. Nomine e autorizzazioni (ruoli privacy)



I ruoli dei vari soggetti, all'interno dell'*organigramma privacy,* possono essere regolamentati da semplici autorizzazioni, come nel caso degli autorizzati al trattamento (tipicamente, dipendenti e collaboratori), o da atti giuridici, come nel caso di responsabili esterni e di contitolari dei trattamenti. I titolari autonomi rivestono il loro ruolo in modo naturale.
Vediamo ora tutti i singoli ruoli e spieghiamo le scelte da effettuare rispetto alle figure più comuni coinvolte nelle attività aziendali:

Titolare dei trattamenti: è la persona/entità giuridica che stabilisce le finalità dei trattamenti e i dati da raccogliere e gestire; è chi mette a disposizione l'*informativa privacy;* è chi ha la responsabilità in caso di violazioni e gestioni illecite dei dati.
Alcuni esempi: l'azienda è titolare dei trattamenti nei confronti dei suoi dipendenti; dei clienti; dei potenziali clienti; dei soggetti ripresi da telecamere di sua proprietà o gestione; potrebbe essere titolare dei trattamenti dei dati dei parenti dei suoi dipendenti, se vengono trattati per motivi di organizzazione del lavoro; dei visitatori, nel momento in cui accedono nella sua sede; degli agenti. Il titolare dei trattamenti lo è "de facto", ma lo deve comunque esplicitare nelle informative esposte.
Ricordiamo che la responsabilità del titolare dei trattamenti "entità giuridica", anche se a responsabilità limitata, ricade sempre sulla persona dell'amministratore o del dirigente, se è ente pubblico o sul rappresentante italiano se è una branch straniera operante nel nostro paese.

Autorizzato ai trattamenti: tipicamente sono i dipendenti e i collaboratori del titolare dei trattamenti che trattano i dati per suo conto e in suo nome. L'atto di nomina ufficiale non è obbligatorio ma fortemente consigliato. In caso di violazioni, la responsabilità per la legge è solo del titolare, ma la nomina può avere una sua valenza internamente all'organizzazione; definisce il ruolo, responsabilizzando la persona incaricata e fornisce le istruzioni di base sui criteri fondamentali dell'utilizzo dei dati personali utilizzati per l'attività aziendale.
Normalmente, in azienda, i dati vengono trattati da receptionist, impiegati amministrativi e commerciali, venditori, addetti al marketing, addetti all'assistenza (in particolare se operano su clientela composta da persone fisiche), manager, ma, in alcuni casi, anche da operai incaricati per alcune mansioni: per esempio, un capo squadra che deve definire turni e/o contattare i suoi colleghi, dovrà gestire numeri telefonici privati e magari geolocalizzare addetti che operano sul territorio.
Riportiamo un esempio di modello di nomina. Precisiamo che i seguenti esempi di nomina (autorizzati e responsabili) devono essere integrati con clausole, informazioni e condizioni, sulla base del tipo di rapporto in essere e del tipo di organizzazione.

Esempio di modello di autorizzazione al trattamento:

MARIO ROSSI

VIA DEL LAVORO, 20

25000 BRESCIA (BS)

P. IVA 23168454869

NOMINA AUTORIZZATO DEL TRATTAMENTO DEI DATI PERSONALI

Spett.le

SIG.RA ROSSI MARIA

VIA BOSCO, 2\A - 24000 REZZATO (BS)

CF: RSSMRA76R70L424Y

LETTERA DI AUTORIZZATO DEL TRATTAMENTO DEI DATI PERSONALI ai sensi e per gli effetti dell'art. 29 del Regolamento 2016/679/UE sulla protezione dei dati personali (nel seguito "GDPR")

In relazione alle attività organizzative e tecniche svolte da ROSSI MARIO per l'applicazione della normativa sulla privacy, Le conferiamo con la presente la designazione di incaricato del trattamento di dati personali e Le confermiamo la Sua autorizzazione, in tale qualità, ad accedere ai medesimi dati e ad eseguire le operazioni di trattamento, tramite strumenti elettronici e documenti anche cartacei, ai fini dello svolgimento dei compiti ed attività a Lei affidati quale Incaricato del trattamento dei dati personali nominato dal Titolare/Responsabile. In qualità di incaricato di trattamento, Lei sarà tenuto ad attenersi scrupolosamente alle istruzioni di seguito fornite, che costituiscono parte integrante del presente incarico, e alle ulteriori istruzioni, anche in materia di sicurezza, riportate negli ulteriori documenti aziendali (es.: regolamenti e manuali operativi) messi a Sua disposizione, nonché alle istruzioni che Le saranno impartite dal Titolare e/o dal responsabile di riferimento. Le ricordiamo, infine, che il mancato rispetto di tali istruzioni potrà comportare la violazione degli obblighi previsti dalla normativa Privacy ed esporre il Titolare, i relativi esponenti ed anche i singoli incaricati a rischi sul piano delle responsabilità e delle sanzioni a livello civile, amministrativo e, nei casi più gravi, anche penale.

* * * * *

Definizioni (art. 4 del GDPR)

“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;

“Dati Particolari/Sensibili”: i dati personali idonei a rivelare l’origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l’adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale e i dati genetici e biometrici utilizzati al fine di identificare in modo univoco una persona fisica;

“Dati giudiziari”: dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti o la qualità di imputato o di indagato;

“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;

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

Istruzioni

In ottemperanza a quanto previsto dal Codice e dal GDPR, Lei dovrà attenersi alle regole relative alla tutela dei dati e delle informazioni, sia in termini di sicurezza, sia in materia di riservatezza.

In particolare, Lei dovrà:

1. trattare i dati in modo lecito e secondo correttezza;

2. trattare i dati personali, in formato sia elettronico che cartaceo, esclusivamente al fine di adempiere alle obbligazioni nascenti dall’incarico conferitoLe e, in ogni caso, per scopi determinati, espliciti e, comunque, in termini compatibili con gli scopi di riservatezza per i quali i dati sono stati raccolti;

3. verificare costantemente la correttezza dei dati trattati e, ove necessario, provvedere al loro aggiornamento;

4. consegnare agli interessati, al momento della raccolta dei dati, il modulo contenente l’informativa di cui all’art. 13 del GDPR, salvo che l’informativa medesima sia stata fornita direttamente dal Titolare o dal Responsabile del trattamento ed eventualmente raccogliere il consenso, ove necessario per le finalità perseguite;

5. trattare i Dati Personali in maniera tale che essi risultino pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Titolare o dal Responsabile del trattamento;

6. conservare i Dati Personali in una forma che consenta l’identificazione dell’interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali gli stessi sono stati raccolti o successivamente trattati;

7. trattare, custodire e controllare i dati, in particolare quelli particolari/sensibili, mediante l'adozione delle misure di sicurezza disposte dal Titolare e/o dal Responsabile del trattamento, al fine di evitare la distruzione, la perdita o l’accesso non autorizzato da parte di terzi, in relazione alle diverse classifiche operative;

8. astenersi dal creare nuove autonome banche dati senza preventiva autorizzazione del Titolare e/o del Responsabile del trattamento;

9. osservare scrupolosamente gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione tanto dei Dati Personali altrui da Lei trattati, quanto delle credenziali di autenticazione a Lei attribuite;

10. garantire, in ogni operazione di trattamento, la massima riservatezza. In particolare, dovrà: a. astenersi dal trasferire, comunicare e/o diffondere i dati al di fuori della Società, salvo preventiva autorizzazione del/la Titolare o dal Responsabile del trattamento; b. svolgere operazioni di trattamento unicamente su dati/banche dati ai quali Lei ha legittimo accesso, nel corretto svolgimento del rapporto di lavoro, e utilizzare a tal fine gli strumenti indicati o messi a disposizione dalla Società; c. osservare, nella fase della raccolta dei dati, la procedura per il rilascio dell'informativa e l'ottenimento del consenso da parte degli interessati;

11. osservare scrupolosamente gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione tanto dei Dati Personali altrui da Lei trattati, quanto delle credenziali di autenticazione a Lei attribuite;

12. in caso di allontanamento, anche temporaneo, dalla postazione di lavoro, verificare che non vi sia possibilità da parte di terzi (anche se Suoi colleghi o comunque appartenenti alla struttura) di accedere ai Dati Personali per i quali era in corso una qualunque operazione di trattamento, sia essa mediante supporto cartaceo o informatico;

13. astenersi dal comunicare a terzi (anche se Suoi colleghi o comunque appartenenti alla struttura) in qualsiasi forma, la/le propria/e credenziale/i di autenticazione, necessaria/e per il trattamento dei Dati Personali con strumenti elettronici;

14. segnalare al Titolare o al Responsabile del trattamento competente in relazione alla Sua funzione eventuali situazioni di rischio per la sicurezza dei dati di cui è venuto a conoscenza (es. la violazione della password, il tentativo di accesso non autorizzato ai sistemi), anche quando riguardino i soggetti esterni autorizzati all'accesso: la Sua collaborazione è fondamentale al fine di colmare eventuali lacune nei sistemi di sicurezza e nelle procedure relative alla tutela dei dati personali;

15. avvisare tempestivamente il proprio responsabile gerarchico qualora si abbia evidenza o anche solo il sospetto che sia in corso una Violazione dei dati personali. Gli obblighi relativi alla riservatezza, alla comunicazione e alla diffusione dovranno essere da Lei scrupolosamente osservati anche in seguito all'eventuale cessazione dall'incarico con la presente le viene assegnato, ovvero dal rapporto di lavoro attualmente in essere con la Società.

Inoltre, La informiamo altresì che:

1. le credenziali di autenticazione a Lei attribuite per consentirLe il trattamento di Dati Personali con strumenti elettronici, saranno disattivate in caso di non uso delle stesse protrattosi per 6 mesi e nel caso in cui Lei dovesse perdere la qualità che Le consente l'accesso ai Dati Personali stessi; 2……

…….inserire condizioni, avvertimenti e informazioni specifiche, in base alla propria organizzazione****

Disposizioni finali

Resta altresì inteso che nessun ulteriore compenso o rimborso le spetterà per l'assunzione della funzione di Incaricato del Trattamento dei dati personali di cui alla presente comunicazione, essendo tale attività parte integrante della mansione. Le comunichiamo che, per qualsiasi ulteriore informazione dovesse occorrerLe in merito alle istruzioni di cui alla presente lettera di incarico, potrà rivolgersi al Titolare del trattamento o al Responsabile del trattamento, come sopra identificato. Sarà cura del Titolare del trattamento o del Responsabile comunicarLe tempestivamente termini e modalità di specifici corsi di formazione, periodicamente organizzati dalla Società. Da ultimo la informiamo che, per l'intera durata del Suo rapporto di lavoro e per un ragionevole periodo di tempo ad esso successivo, Lei è tenuto a mantenere la massima riservatezza sui Dati e sulle informazioni di cui abbia avuto conoscenza nello svolgimento delle attività affidateLe, non solo nei rapporti con terzi rispetto all'azienda ma anche nei rapporti con i colleghi di lavoro.

Distinti saluti.

Luogo e Data: _____

Il Titolare/Responsabile del trattamento dei dati per presa visione

Firma dell'Incaricato/a

_____ _____

Responsabile esterno: è la persona/entità giuridica, che opera tipicamente, al di fuori dell'organizzazione del titolare dei trattamenti, trattando i dati per conto di quest'ultimo. Alcuni esempi di responsabili esterni: consulenti del lavoro, commercialisti, società di assistenza informatica, società di medicina del lavoro, consulenti per la sicurezza, etc. nel momento in cui trattano i dati dei dipendenti, dei clienti o di altri soggetti in relazione con il titolare dei trattamenti.

Ci sono alcuni soggetti, ad esempio, le banche, le assicurazioni, le organizzazioni sindacali, i gestori di fondi pensione e i medici competenti (quando sono liberi professionisti), che rivestono sempre il ruolo di *titolari autonomi dei trattamenti,* cioè di soggetti "alla pari" del titolare dei trattamenti e che, quindi, non vanno nominati con atti giuridici.

Esempio di nomina di responsabile esterno

MARIO ROSSI

VIA DEL LAVORO, 20

25000 BRESCIA (BS)

P. IVA 23168454869

Accordo di NOMINA A RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI

Spett.le COMMERCIALISTA DEI COMMERCIALISTI S.R.L.

VIA DEI COMMERCIALISTI, 21

26000 DESENZANO (BS)

P.IVA: 15789548632 - CF: 15789548632

Oggetto: Accordo sul trattamento dei Dati Personali connesso all'erogazione dei servizi in favore di ROSSI MARIO, Titolare del trattamento dei dati personali, ai sensi della vigente normativa sulla protezione dei dati personali art. 28 del Regolamento 2016/679/UE (nel seguito anche "GDPR")

Egregi Signori,

facciamo seguito alle intese intercorse per confermarVi quanto segue.

Premesso che:

a) è in corso un rapporto contrattuale tra le nostre società (per brevità detto anche il “Contratto”), finalizzato all’erogazione, in favore di ROSSI MARIO di servizi relativi al trattamento dei dati personali denominato "Gestione Amministrativo - Contabile interna" (per brevità detti anche “Servizi”) da parte di COMMERCIALISTA DEI COMMERCIALISTI S.R.L. (per brevità, detta anche “Fornitore” e, congiuntamente con Titolare, le “Parti”);

b) ai sensi della vigente normativa europea ed italiana in materia di protezione dei dati personali (la “Normativa Privacy”), l’esecuzione dei Servizi comporta, da parte di COMMERCIALISTA DEI COMMERCIALISTI S.R.L., il trattamento di dati personali per conto di ROSSI MARIO quale “Titolare”; c) a mezzo della presente le Parti intendono disciplinare il trattamento dei dati personali effettuato dal Fornitore quale Responsabile del trattamento nell’esecuzione dei Servizi di cui al Contratto, ai sensi della normativa sulla protezione dei dati personali. MARIO ROSSI VIA DEL LAVORO, 20 25000 BRESCIA (BS) P. IVA 23168454869

Tutto ciò premesso, tra le Parti si conviene e stipula quanto segue:

1. Le Parti, con riferimento alle attività di trattamento dei dati personali connesse alla fornitura dei Servizi di cui al Contratto, concordano che tali attività sono svolte dal Fornitore COMMERCIALISTA DEI COMMERCIALISTI S.R.L. per conto di ROSSI MARIO quale Titolare del trattamento e che il Fornitore agisce in qualità di Responsabile di tale trattamento, ex art. 28 del GDPR.

2. Le Parti si danno reciprocamente atto che la fornitura dei Servizi comporta il trattamento dei dati personali descritto come contrattualmente convenuto come meglio indicato dal Contratto/Accordo del quale il presente Atto costituisce parte integrante nonché come descritto nel seguito. 3. Il Fornitore, in qualità di Responsabile, conferma di presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento risponda ai requisiti prescritti al fine di garantire la tutela dei dati personali e i diritti degli interessati.

4. il Fornitore si impegna a rispettare gli obblighi che le disposizioni del GDPR e del D. lgs. 196/03, come modificato dal D. lgs. 101/18, pongono direttamente a carico del Responsabile del trattamento:

a) effettuare le operazioni di trattamento dei suddetti dati personali nel pieno rispetto dei principi e delle disposizioni della vigente normativa sulla protezione dei dati personali ed esclusivamente ai fini dell’esecuzione dei Servizi, secondo le modalità, procedure e modulistiche via via indicate dal Titolare;

b) trattare i dati personali soltanto sulla base delle documentate istruzioni fornite da ROSSI MARIO quale Titolare, anche in caso di eventuale trasferimento di dati personali verso soggetti stabiliti in Paesi al di fuori della UE, che potrà essere effettuato solo previa autorizzazione del Titolare medesimo e sulla base delle relative istruzioni, adottando le adeguate garanzie secondo la vigente normativa europea e nazionale di riferimento, garanzie di cui andrà mantenuta adeguata documentazione da fornire, ove richiesto, a ROSSI MARIO;

c) adottare tutte le misure richieste per la sicurezza del trattamento, ai sensi dell’art. 32 del GDPR nonché dei provvedimenti prescrittivi del Garante in tema di sicurezza dei dati ed amministratori di sistema fino alla loro eventuale modifica, sostituzione ed abrogazione, successivamente al 25 maggio 2018;

d) assistere il Titolare nel garantire il rispetto, per quanto di relativa competenza, degli obblighi in tema di sicurezza, notifica all’Autorità per la protezione dei dati personali (nel seguito “Garante”) di eventuali violazioni di dati personali e, se del caso, loro comunicazione agli interessati, nonché di valutazione d’impatto sulla protezione dati ed eventuale consultazione preventiva, ai sensi degli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione dello stesso Responsabile, nonché delle documentate istruzioni via via impartite dal Titolare in relazione all’adempimento dei suddetti obblighi;

e) individuare le persone autorizzate al trattamento dei dati personali (gli Incaricati), che operano sotto l’autorità del medesimo Fornitore, nonché adottare le misure volte a (i) garantire l’assunzione da parte di tali persone di idonei obblighi di riservatezza in ordine ai dati personali trattati, (ii) fornire loro adeguate e documentate istruzioni circa il rispetto, in particolare, delle misure per la sicurezza dei dati e (iii) vigilare sulla osservanza, da parte delle persone autorizzate, delle istruzioni impartite per il trattamento dei dati personali e delle vigenti disposizioni normative in materia di protezione dei dati personali;

f) assicurare, ai fini della corretta applicazione della vigente normativa sulla privacy, il costante monitoraggio degli adempimenti e delle attività effettuati da chi opera sotto la propria autorità (se applicabili: fornire l'informativa, raccogliere il consenso, l'elaborazione ed archiviazione, la comunicazione e la diffusione, etc.) in relazione alle operazioni di trattamento di competenza; MARIO ROSSI VIA DEL LAVORO, 20 25000 BRESCIA (BS) P. IVA 23168454869

g) informare periodicamente il Titolare, su richiesta di quest'ultimo, in ordine all'attività svolta, sia sotto il profilo del trattamento, sia sotto il profilo della sicurezza dei dati;

h) conservare i dati in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti e successivamente trattati;

i) inviare al Titolare previa apposita richiesta scritta, al momento della cessazione delle operazioni di trattamento o anche antecedentemente in caso di specifica richiesta del Titolare, la documentazione comprovante l'avvenuta esecuzione degli adempimenti privacy;

j) informare prontamente il Titolare di ogni questione rilevante ai fini della presente nomina, quali a titolo indicativo:

(i) istanze di interessati;

ii) richieste del Garante;

(iii) violazioni o messa in pericolo della riservatezza, della completezza o dell'integrità dei dati personali.

k) fornire per quanto di competenza la massima collaborazione al Titolare in caso di istanze avanzate da parte degli interessati, ex artt. dal 15 al 22 del GDPR, le cui informazioni sono trattate in esecuzione dei Servizi o in caso di accertamenti o ispezioni effettuate da parte del Garante, nonché in caso di qualsiasi controversia avente ad oggetto la normativa a tutela dei dati personali;

l) garantire per quanto di competenza l'esecuzione di ogni altra operazione richiesta o necessaria per ottemperare agli obblighi derivanti dalle disposizioni di legge e/o da regolamenti vigenti in materia di protezione dei dati personali;

m) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente Atto ed alla vigente Normativa Privacy, nonché consentire e contribuire alle attività di revisione, comprese le ispezioni che il Titolare (con preavviso minimo di 5 giorni), direttamente o avvalendosi di terzi, potrà effettuare per verificare la puntuale osservanza di quanto previsto dalla vigente normativa in materia di protezione dei dati personali nonché delle proprie indicazioni.

5. Con riferimento al trattamento dei dati personali connesso alla fornitura dei Servizi di cui al Contratto, ROSSI MARIO autorizza il Fornitore ad avvalersi degli ulteriori responsabili informando tempestivamente il Titolare, che potrà manifestare la sua opposizione entro 15 giorni dal ricevimento di tale comunicazione. Il Responsabile si impegna a che tali ulteriori responsabili posseggano competenze, conoscenze ed esperienze sufficienti per mettere in atto misure tecniche e organizzative idonee a garantire il rispetto delle disposizioni del GDPR. Il Responsabile si impegna, nell'ambito dei contratti od accordi stipulati con gli ulteriori responsabili, a:

(i) vincolare contrattualmente gli ulteriori responsabili al rispetto degli stessi obblighi in materia di protezione dei dati personali assunti dal Responsabile nei confronti del Titolare, ove applicabili e pertinenti rispetto alle attività a questi ultimi affidate;

(ii) custodire copia dei predetti contratti, accordi o documenti disciplinanti gli obblighi in materia di protezione dei dati personali, sottoscritti per presa visione ed accettazione da parte degli ulteriori responsabili e fornirne copia al Titolare, su sua richiesta;

(iii) assumere nei confronti del Titolare ogni responsabilità in ordine al rispetto dei predetti obblighi da parte degli ulteriori responsabili;

6. L'esecuzione delle attività di cui al presente accordo non originano alcun diritto del Responsabile a percepire compensi ulteriori rispetto a quanto previsto per i Servizi.

7. Il Responsabile si impegna a tenere indenne il Titolare da ogni responsabilità, costo, spesa o altro onere, discendenti da pretese, azioni o procedimenti di terzi a causa della violazione, da parte del Responsabile (o di suoi dipendenti o collaboratori ovvero degli ulteriori responsabili), degli obblighi a suo carico in base alla presente e/o della violazione delle prescrizioni di cui alla vigente normativa in materia di protezione dei dati personali. MARIO ROSSI VIA DEL LAVORO, 20 25000 BRESCIA (BS) P. IVA 23168454869

8. Alla cessazione per qualsiasi causa dei Servizi, il Responsabile sarà tenuto, a discrezione del Titolare:

(i) a restituire al Titolare i dati personali oggetto del trattamento oppure

(ii) a provvedere alla loro integrale distruzione, salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge ad altri fini (contabili, fiscali, ecc.). In entrambi i casi il Responsabile provvederà a rilasciare al Titolare apposita dichiarazione per iscritto contenente l'attestazione che presso il Responsabile non esiste alcuna copia dei dati personali e delle informazioni di titolarità di ROSSI MARIO, fatti salvi i casi in cui la conservazione dei dati sia richiesta da norme di legge ad altri fini (contabili, fiscali, ecc.). Il Titolare si riserva il diritto di effettuare controlli e verifiche volte ad accertare la veridicità della dichiarazione.

9. La presente nomina va intesa come se fosse stata effettuata all'inizio del rapporto contrattuale tra le nostre Società ed avrà durata fino alla cessazione, per qualsivoglia motivo, dello stesso.

…….inserire condizioni, avvertimenti e informazioni specifiche, in base alla propria organizzazione****

Luogo e data, _____

_____

ROSSI MARIO

Per presa visione e accettazione

_____

Luogo e data di sottoscrizione

_____

COMMERCIALISTA DEI COMMERCIALISTI S.R.L.

Contitolare: si riferisce a quelle entità che, insieme ad altre, trattano i dati di soggetti interessati con lo scopo di fornire prodotti e/o servizi in abbinamento. Alcuni esempi possono essere rappresentati dai servizi dei tour operator insieme a quelli di compagnie aeree e alberghi, se concorrenti a fornire un pacchetto di viaggio; un altro esempio, può essere quello di una banca e di una società assicurativa, nel momento in cui una polizza fosse strumentale all'erogazione di un finanziamento.
La *contitolarità* è stabilita con un atto giuridico che deve definire chiaramente le rispettive responsabilità dei trattamenti effettuati.

Altre nomine:

Amministratore di sistema: è la persona interna o esterna all'organizzazione che si occupa di sovrintendere alle operazioni di sicurezza e di buona gestione dell'infrastruttura informatica; si occupa di ottimizzare i sistemi, di aggiornare i software, di gestire le password, etc. Era una figura obbligatoria nella vecchia normativa. Con l'attuale regolamento non è più obbligatoria ma fortemente consigliata, in quanto, una sua mancanza potrebbe essere interpretata come un'insufficiente applicazione delle misure idonee.

Designato alla privacy: è la persona, interna all'azienda, che si occupa di tutte le buone pratiche relative alla privacy in azienda: mantiene i contatti con i consulenti, si occupa della gestione dei consensi privacy e delle richieste dei soggetti interessati, mette a disposizione le informative e così via.
Per ottemperare all'applicazione di misure organizzative idonee, può essere necessario nominare dei designati, all'interno dell'azienda, che si occupano della corretta gestione dell'impianto di registrazione della videosorveglianza, della conservazione delle chiavi degli armadi contenenti dati personali, etc, anche se non sono figure imposte dal regolamento.

Destinatari esterni: generalmente si tratta di entità pubbliche come Inail, Inps, Agenzia delle Entrate, etc., che per normative nazionali sono abilitati a ricevere e trattare dati personali. Un esempio è anche la Pubblica Sicurezza, quando riceve i dati dei clienti degli alberghi. Possono essere anche strutture private, come le banche (nel caso in cui devono emettere Riba o bonifici verso terzi) o società di recupero del credito o avvocati, quando operano per conto del titolare dei trattamenti, verso soggetti terzi.
Non sono necessarie nomine.

Titolari autonomi: sono generalmente entità giuridiche che trattano dati di altri titolari dei trattamenti, ma per finalità proprie ben definite. Un esempio, sono le assicurazioni o i gestori di fondi pensione quando gestiscono le adesioni dei dipendenti del titolare dei trattamenti. Un altro esempio calzante è rappresentato dai soggetti coinvolti quando si accende un mutuo con una banca e l'assicurazione sul bene oggetto del mutuo con una compagnia assicurativa.

Step 4. Analisi dei rischi privacy e implementazione misure adeguate.

L'analisi dei rischi privacy è da intendersi come un'analisi rispetto alla capacità di conservazione delle 3 caratteristiche essenziali del dato: riservatezza, integrità, disponibilità e la gravità delle conseguenze nel caso di una loro perdita.
La riservatezza può essere inficiata da un episodio di violazione informatica, dall' invio di una mail al destinatario sbagliato, da un furto, dalla diffusione illegale di dati, etc.; l'integrità può non essere più tale, nel caso di infezione di virus informatici, di file danneggiati, da procedure scorrette o problemi di software; la disponibilità viene a mancare se, per esempio, conservando dei dati in un sistema cloud, per qualche problema tecnico, si interrompe la connessione alla linea dati/internet; se per problemi di sistema non fosse possibile accedere al gestionale.
La tabella sottostante, aiuta a valutare e rappresentare graficamente i livelli di rischio per ogni situazione. Chi la compila, deve analizzare tutte le possibili conseguenze di un evento relativo ai dati di un soggetto, valutandone i rischi.
Alcuni esempi:
a) Perdita riservatezza.
Documenti trattati: documenti di identità e buste pag. Rischio: furto di identità e truffe. Livello di rischio sulla persona: alto;
Documenti trattati: numeri di telefono pubblici di fornitori. Rischio: contatti da parte di ignoti a fornitori dell'azienda. Livello di rischio sulla persona: basso.
Perdita disponibilità.
b) Documenti trattati: mail di clienti. Cosa non è possibile fare senza quegli indirizzi per quel trattamento? Non è possibile inviare mail promozionali. Livello di rischio sulla persona: basso.
Documenti trattati: mail di clienti. Cosa non è possibile fare senza quegli indirizzi per quel trattamento? Non è possibile inviare dei referti medici. Livello di rischio sulla persona: alto.

Tab. 5
ANALISI DEI RISCHI

Trattamento:…	Rischio basso	Rischio medio	Rischio alto
Riservatezza			
Integrità			
Disponibilità			

E' consigliabile realizzare tante tabelle quanti sono i gruppi di trattamento:
gestione clienti; gestione personale; gestione commerciale; etc.

Sulla base dei livelli di rischio risultanti si decide che strategia applicare per la protezione dei dati.
Se vengono trattati dati che possono dar luogo ad un elevato livello di rischio, in termini di riservatezza, sarà opportuno ipotizzare l'implementazione di: sistemi anti intrusione, firewall, antivirus, crittografia dei dati, password complesse, sistemi di log management, etc.
Un alto livello di rischio per problemi di integrità e disponibilità si potrebbe risolvere con l'implementazione di sistemi di ridondanza e back up incrementali a scansione frequente, così da garantire sempre la pronta disponibilità del dato quando serve.
Il titolare dei trattamenti ha la più ampia libertà di azione, fermo restando che, in caso di ispezione, sta a quest'ultimo dimostrare di aver fatto il possibile per proteggere i dati personali trattati.
Si consiglia di analizzare insieme al proprio fornitore di sistemi informatici e all'amministratore di sistema, il livello di sicurezza raggiungibile, i costi e le implicazioni in termini di processi aziendali, così da conciliare la capacità reddituale dell'impresa con efficaci provvedimenti a tutela dei dati da proteggere, che, ricordiamo, sono i dati personali, se guardiamo al Gdpr, ma sono tutti i dati aziendali rilevanti, se consideriamo la tutela della propria impresa.

Le misure *idonee*, come riportato nel regolamento, consistono in misure *tecniche e organizzative*, quindi, il titolare dei trattamenti, dovrà implementare, oltre alle componenti tecnologiche hardware e software, quelle inerenti i processi, le policy e la formazione obbligatoria.

Entriamo nel dettaglio, elencando alcuni esempi di processi implementabili in azienda:

- raccolta del consenso effettuabile tramite mail, prima dell'invio di materiale promozionale;
- codice di comportamento per l'utilizzo degli strumenti informatici dei dipendenti, come indicato dal datore;
- eliminazione dei dati cartacei, una volta terminata la loro funzione, per mezzo di un distruggidocumenti;
- formazione del personale in tema di privacy e sicurezza informatica;
- definire delle cartelle su server separati e protetti suddivise per soggetti interessati (dati clienti; dati dipendenti; dati fornitori; etc.), con specifiche autorizzazioni di accesso per le persone designate a quel trattamento;
- analisi sicurezza del portale web che raccoglie i dati dei clienti.
- ……..

E' consigliabile effettuare una disamina dei dati personali trattati, identificando quelli più sensibili riguardanti quindi il reddito, i documenti personali, la profilazione, i dati giuridici, etc., predisponendo delle tutele e delle protezioni maggior, cercando di trattarli nel modo più ridotto possibile, diminuendone al massimo la diffusione verso altri soggetti.

L'analisi dei rischi e le scelte effettuate rispetto ai sistemi tecnologici di sicurezza da implementare, sono da conservare presso la propria sede e da tenere a disposizione in caso di ispezioni.

Step 5. Redazione della DPIA (Data Protection Impact Assessment – Valutazione di Impatto Privacy).

Alcuni particolari trattamenti di dati in azienda richiedono la redazione di uno specifico documento di valutazione rischi, chiamato "Valutazione di Impatto Privacy".

Questo documento si deve redigere quando vengono effettuati trattamenti automatizzati; trattamenti di dati molto sensibili; dati di soggetti appartenenti a fasce deboli (disabili, minori, anziani, etc.); trattamenti che incidono sull'accesso a servizi o contratti; trasferimenti di dati extra UE; decisioni automatizzate; trattamenti effettuati tramite strumenti di innovazione tecnologica; valutazioni e scoring; raffronto di dati; geolocalizzazione; monitoraggio sistematico.
Le linee guida prevedono che la DPIA debba essere effettuata quando sussistano almeno due delle condizioni sopra esposte.
Per esempio, un impianto di videosorveglianza la richiede, in quanto effettua un monitoraggio costante e tratta dati particolari (immagini) di una moltitudine di soggetti, anche fasce deboli (lavoratori, disabili, etc.).
Lo stesso vale per un impianto gps atto a geolocalizzare i veicoli condotti dal personale della propria azienda.
La DPIA deve essere effettuata prima del trattamento in oggetto e deve ripetuta almeno ogni tre anni.

Di seguito, i principali contenuti della valutazione d'impatto:

1. elenco dei soggetti (nome, cognome, ruolo in azienda, ruolo specifico in tema di privacy/sicurezza dati) coinvolti nella redazione del documento;
2. data, luogo della redazione del documento;
3. descrizione dei trattamenti in oggetto, delle finalità e, riportare, per i trattamenti oggetto della DPIA, le seguenti informazioni: finalità; basi giuridiche (vedi sezione specifica dedicata alle basi giuridiche) e se previsto, la motivazione dell'applicazione della base giuridica del" legittimo interesse" (per esempio, si descrive l'impiego della videosorveglianza allo scopo di tutelare il patrimonio); diffusione dei dati ai vari soggetti previsti; altre normative di riferimento (per esempio, la legge 300/1970 per il ruolo del diritto del lavoro, in caso di trattamento di videosorveglianza);
4. valutazione di necessità e proporzionalità dei trattamenti (per esempio, si giustifica il fatto di conservare le immagini video per una settimana perché, in un negozio, ci si può accorgere di un furto alcuni giorni dopo);
5. valutazione di necessità e proporzionalità dei trattamenti (per esempio, si giustifica il fatto di conservare le immagini video per una settimana perché, in un negozio, ci si può accorgere di un furto alcuni giorni dopo);
6. valutazione rischi, diritti e libertà dei soggetti (per esempio, se malintenzionato accedesse alle immagini delle telecamere in luogo di lavoro dove si tratta denaro contante, potrebbe controllare le abitudini del personale e pianificare una rapina, oppure, la violazione di un sistema contenente dati biometrici di molte persone potrebbe consentire una profilazione di massa con dati sensibili);
7. valutazione delle misure di sicurezza applicate e decisione di implementarne di nuove, se necessario, sempre rispettando il regolamento.

Se l'esito di una valutazione d'impatto non fornisce una soluzione alle possibili minacce ai diritti fondamentali e alle libertà dei soggetti interessati, il trattamento deve essere autorizzato dall'ufficio dell'autorità del Garante della privacy.

Step 6. Analisi dei dati trattati e definizione delle basi giuridiche definite.

Iniziamo a spiegare cosa si intende per *basi giuridiche*: sono le condizioni legali che rendono lecito il trattamento dei dati personali.
Spesso, viene utilizzato il *consenso* per giustificare la raccolta di dati che, in realtà, avrebbero una base giuridica differente. Quante volte ci è stato chiesto il consenso per la richiesta dei dati di fatturazione di un bene o servizio? E' uno dei casi di errata applicazione delle basi giuridiche.
La base giuridica per un determinato trattamento di dati dovrà essere riportata nel *registro dei trattamenti*, che vedremo in seguito, e nelle *informative* che andremo a redigere e a rendere pubbliche, tramite l'apposizione negli uffici, la pubblicazione sul sito, etc.
Elenchiamo, di seguito, le basi giuridiche perviste per il trattamento dei dati personali con alcuni esempi di applicazione:

il consenso.
Il consenso, espresso dal soggetto ai quali i dati sono riferiti, rappresenta la base giuridica da applicare per le seguenti finalità (esempi più comuni): marketing/promozionali. Ad es.: la richiesta di una mail o di un numero di cellulare con la finalità di inviare comunicazioni promozionali; Il trattamento e la diffusione ad altre entità dei dati trattati, per finalità non strettamente legate al contratto stipulato. Ad esempio, il nominativo di un visitatore che si è recato presso gli uffici di un'azienda o i dati di un cliente, per l'invio di newsletter; la profilazione di clienti (utilizzo di una serie di informazioni su un individuo, che, una volta integrate, creano un "profilo" di utente/cliente, al

quale formulare proposte di acquisto specifiche. In genere, le informazioni e i dati richiesti comprendono: informazioni relative alle abitudini di vita; abitudini di acquisto; personali; genere; età; etc.); il trattamento di tutti i dati che, pur rappresentando una "comodità" per la fornitura di un servizio (sia per il cliente, che per il fornitore) non sono strettamente indispensabili (per esempio, il numero di cellulare privato); il trattamento di dati particolari (sanitari; giudiziari; etc.); diffusione di dati personali verso paesi esterni all' UE, ad esclusione dei paesi extra UE per i quali esistono accordi bilaterali o di "adeguatezza" (vedi elenco disponibile presso il Garante della privacy).

Esecuzione del contratto.

Da utilizzare per il trattamento di tutti quei dati necessari, ad esclusione dei dati particolari, senza i quali una fornitura non potrebbe avere luogo. Se, ad esempio, fosse necessario effettuare una riparazione in un'abitazione, sarà necessario ottenere l'indirizzo della stessa e magari un recapito telefonico. Vale anche rispetto all'assunzione di un collaboratore.

L'obbligo legale.

Viene applicato quando una legge, un decreto o un regolamento impone quello specifico trattamento. Ad esempio, i dati raccolti da un hotel al momento del soggiorno di un ospite o i dati trattati da un'azienda al momento dell'assunzione di un dipendente.

Salvaguardia interessi vitali.

La salvaguardia di interessi vitali di uno o più soggetti, è, giustamente, una base giuridica che legittima, in casi di forza maggiore, il trattamento di dati personali.

Compiti di interesse pubblico connesso all'esercizio di pubblici poteri.

Riguarda fondamentalmente dati personali trattati nell'ambito pubblico**.**

Legittimo interesse del titolare dei trattamenti.

Viene applicato secondo un principio di bilanciamento di interesse del titolare e libertà e diritti del soggetto interessato. Per esempio, è la base giuridica che rende lecita la videosorveglianza per motivi di sicurezza del patrimonio o di sicurezza sul lavoro o il trattamento dei dati di contatto di un debitore.

Consigliamo di effettuare un'ampia analisi dei dati trattati, verificando, per ogni soggetto interessato, quali dati vengono trattati, con quali basi giuridiche e con alcune informazioni fondamentali, come riportato nella prossima tabella. In questo modo, si avrà a disposizione una serie di dati che saranno indispensabili per la redazione dei documenti successivi.

Tab. 5

SCHEMA DI ANALISI DEI DATI TRATTATI PER SOGGETTO (ALCUNI ESEMPI)

Si consiglia di realizzare uno schema, durante l'attività di analisi dei dati trattati, con le informazioni sotto riportate. A fine lavoro si avrà pronto uno schema per la compilazione del "registro dei trattamenti".

Soggetto interessato	**Tipo di dato trattato**	**Finalita'**	**Base giuridica**	**Diffusione dati extra ue**	**Diffusione dati a terzi**	**Tempi di conservazione**	**Chi, come,dove raccoglie il dato e come e dove viene conservato**
cliente	cellulare	contatto	consenso	no	no	Tempo esecuzione contratto	L'agente;durante la visita;inserisce nel gestionale
cliente	mail	marketing	consenso	no	consulente marketing	5 anni	Tramite mail;archivio generale…
cliente	indirizzo	spedizione merce	esecuzione contratto	no	corriere	Tempo esecuzione contratto	Impiegato; al telefono;nel gestionale

dipendente	cud	Dichiarazione dei redditi	legge nazionale	no	commercialista	Tempo esecuzione contratto	Redatto dall'uff del personale; conservato nell'armadio 1
dipendente	immagine	videosorveglianza	legittimo interesse	no	no	Una settimana	Telecamere;vdr
fornitore	cellulare	contatto	esecuzione contratto	no	no	Tempo esecuzione contratto	Ufficio acquisti; rubrica fornitori; server 1

La tabella è fondamentale per ottenere tutti i dati che si dovranno inserire nel *registro dei trattamenti* e nelle specifiche *informative privacy* da rendere disponibili ai soggetti interessati.

Step 7. Il DPO (Data Protection Officer – Responsabile della Protezione dei Dati).

Cos'è e in cosa consiste il ruolo del DPO

Il DPO o RPD, secondo l'acronimo italiano (Responsabile Protezione Dati), è un professionista, interno o esterno all'organizzazione (può essere anche un'entità giuridica, ma deve sempre definita una persona fisica di riferimento), che ha la funzione di relazionarsi con il management e con tutte le divisioni aziendali allo scopo di: assicurare la corretta applicazione di tutte le misure tecniche ed organizzative idonee alla protezione dei dati e le procedure riguardanti il tema della privacy; effettuare audit di verifica degli adeguamenti alla normativa; effettuare la formazione obbligatoria; fungere da collegamento tra l'azienda e i soggetti interessati e tra l'azienda e l'ufficio del Garante della privacy; effettuare la *valutazione d'impatto privacy*; assicurare l' esercizio dei diritti dei soggetti interessati.
L'incarico non può essere affidato ad un manager, a persone dell'azienda o all'amministratore di sistema, in quanto, avendo un ruolo attivo nel trattamento dei dati del titolare dei trattamenti, si configurerebbe un conflitto di interessi.
Il DPO deve poter partecipare ai cda nei quali si discute di tematiche riguardanti la privacy e deve essere sempre informato sui processi aziendali che coinvolgono il trattamento di dati personali e deve poter disporre di un budget per l'applicazione delle misure necessarie all'adeguamento alla normativa.
La nomina del DPO va notificata all'ufficio del Garante al momento della nomina.
Tutte le informative riguardanti il trattamento dei dati personali devono riportare il nome di chi riveste il ruolo di DPO e i suoi dati di contatto per il pubblico.
Il DPO può essere un dipendente, dedicato solo a quella mansione, o un professionista esterno che svolge il ruolo in outsourcing.

Quando deve essere nominato il DPO
Questo manuale si rivolge ad aziende e professionisti che, generalmente, non hanno necessità di nominare un DPO. Tuttavia, non è raro incontrare imprenditori a capo di piccole realtà che, per particolari attività aziendali, sono tenuti a nominarlo. Per questi è consigliata una consulenza specifica, in quanto, una simile esigenza, presuppone una complessità d'intervento difficilmente esauribile con un manuale.

Le condizioni che rendono obbligatoria per legge la nomina del DPO sono le seguenti:

- svolgere un'attività principale che prevede un sistematico monitoraggio su *larga scala* di soggetti interessati;
- svolgere un'attività principale che prevede un sistematico trattamento su *larga scala* di dati particolarmente sensibili (dati sulla salute, sulle idee politiche e religiose, dati giudiziari, etc.);
- svolgere un'attività nell'ambito della Pubblica Amministrazione.

Definizione di "trattamento su *larga scala*"
Non esiste una definizione precisa e inequivocabile, in quanto, dipende dall'incidenza del numero di soggetti coinvolti in relazione all'area territoriale nella quale si svolge l'attività. Per esempio, un migliaio di soggetti sul territorio nazionale non è "larga scala", mentre lo diventa in un comune di 5000 abitanti. Inoltre, dipende anche dalla continuità di dati particolari trattati. Se, per esempio, si svolge attività di

recupero del credito, analisi mediche o altre attività che implicano il trattamento di dati particolari, ad un certo numero di soggetti, anche non molto elevato, è consigliabile nominare il DPO. Per valutare la necessità della nomina di un DPO, in alcuni casi, è consigliabile effettuare un'analisi più approfondita.

I soggetti che operano in libera professione (medici, consulenti, etc.) non hanno l'obbligo di nomina del DPO, anche se trattano una certa quantità di dati particolari, a meno che non lavorino in associazione con altri professionisti, generando un impatto sui soggetti, nel territorio, di notevole entità.

Step 8. Il/i registro/i dei trattamenti.

Deve essere redatto obbligatoriamente da chi ha almeno un dipendente, in forma ridotta, da chi ha 250 dipendenti, in forma completa, come chi tratta dati particolari (sanitari, giudiziari, etc.).
Il documento deve essere redatto sia dai titolari dei trattamenti, sia dai responsabili esterni; aggiornato periodicamente e conservato in formato cartaceo o elettronico, a disposizione delle autorità, in caso di ispezione.
E' consigliabile considerare i trattamenti come "macrocategorie", per esempio, "trattamento gestione personale" o "trattamento clienti per esecuzione contratto", piuttosto che "trattamento videosorveglianza" e, per ogni categoria, riportare le informazioni sotto riportate:

- nome e dati di titolare, contitolare, responsabile protezione dati (se applicabile);
- finalità del trattamento;
- basi giuridiche;
- categorie soggetti interessati e categorie tipologie di dati trattati;
- autorizzati e responsabili del trattamento;
- categorie di destinatari dei dati come, ad esempio, paesi terzi od organizzazioni internazionali;
- documentazione garanzie per trasferimenti verso paesi terzi (extra UE);
- tempi di conservazione dei dati;
- sintetica descrizione delle misure idonee adottate per la sicurezza del trattamento.

Esempio di registro dei trattamenti "titolare":

Registro dei trattamenti del titolare (art.30 del Gdpr) Società Pippo Srl **Redatto il 10 aprile 2020**	**Gruppi di trattamenti**		
	Gestione personale	**Gestione clienti**	**Videosorveglienza**
Titolare	Pippo Srl	Pippo Srl	Pippo Srl
Contitolare	-	-	-
Dpo	Mario Rossi	Mario Rossi	Mario Rossi
Finalità trattamento	Adempimenti relativi al contratto; adempimenti di legge; welfare;….	Adempimenti relativi al contratto; contatto commerciale; assistenza;…	Sicurezza del patrimonio; sicurezza del lavoro;….
Basi giuridiche	Esecuzione del contratto	Esecuzione del contratto; consenso esplicito (per il	Legittimo interesse del titolare

		marketing); consenso per l'utilizzo del numero di cellulare come contatto.	
Soggetti interessati	Dipendenti; collaboratori	Clienti; potenziali clienti	Dipendenti; collaboratori; agenti; visitatori;..
Categorie di dati	Dati fiscali-contributivi; dati di contatto; dati economici;…	Dati di contatto; dati fiscali; ..	Dati biometrici (immagini filmate)
Autorizzati (collaboratori)	Franco Bianchi; Giulia Verdi	Giulio Gialli	Luigi Viola
Responsabili esterni	Dott Neri (consulente lavoro); Sicur Srl (sicurezza del lavoro); …	Giuseppe Grigio (agente); Studio Com (commercialista)	Sicurvideo Srl (società di sicurezza)
destinatari	Inps; Agenzia delle Entrate; banca..	Banche;	-
Diffusione verso paesi non Ue	Dati di dipendenti in missione: Iran; Russia. Finalità: il visto d'ingresso e l'hotel. Garanzie: clausole contrattuali; necessità di esecuzione del contratto; accordi vincolanti; …	-	-
Tempo di conservazione	Durata del contratto – 10 anni per legge	Durata del contratto – 10 anni per legge (dati fiscali)	48 ore
Misure di sicurezza	Armadi sotto chiave; server e pc con sistema antintrusione; firewall;..	Armadi sotto chiave; server e pc con sistema antintrusione;…	Videoregistratore sotto chiave con password complessa

Il registro potrebbe comprendere altri trattamenti e maggiori specifiche per ogni singolo trattamento a seconda della tipologia di organizzazione alla quale si riferisce.

Step 9. Le informative e i consensi.

Informative e consensi privacy rappresentano certamente gli elementi più conosciuti e più evidenti del tema della privacy. Non sempre sono realizzati e utilizzati come indicato dal regolamento vigente.
Ma vediamo, nel dettaglio le caratteristiche di questi due documenti.

9.a) Informative privacy

Le informative privacy soddisfano l'esigenza di trasparenza, richiesta dalla normativa, che impone al titolare dei trattamenti di informare i soggetti interessati, in modo trasparente, tutte le implicazioni e le modalità di trattamento dei suoi dati e i diritti che può far valere.
Di seguito, alcuni concetti fondamentali.
Le informative privacy devono:

- essere facilmente accessibili e leggibili se in presenza di trattamenti di dati personali (anche quando non sono sensibili);
- essere specifiche per alcune categorie di soggetti e per gruppi di trattamenti effettuati (informativa dipendenti; informativa

clienti; informativa videosorveglianza; informativa fornitori; informativa sito web; etc.);
- contenere tutte le informazioni previste dalla normativa;
- essere consegnate o rese disponibili quando richiesto;
- contenere i dati di contatto del titolare dei trattamenti; del responsabile e del Dpo, se presente.

I contenuti dell'informativa devono essere i seguenti:

- nome o ragione sociale e recapiti del: titolare dei trattamenti; eventuale responsabile; eventuale Dpo;
- origine; finalità; base giuridica e natura dei dati trattati;
- categorie di destinatari dei dati ed eventuale diffusione all'estero degli stessi;
- modalità; logiche del trattamento e tempi di conservazione dei dati;
- diritti dei soggetti interessati (rettifica; cancellazione; limitazione; portabilità; opposizione e ricorso al Garante della Privacy);
- conseguenze del mancato trattamento dei dati.

Di seguito, un esempio di informativa privacy "clienti":

MARIO ROSSI
VIA DEL LAVORO, 20
25000 BRESCIA (BS)P. IVA 23168454869

Informativa sul trattamento dei dati personali dei Clienti

Ai sensi degli artt. 13 e 14 del Regolamento 2016/679/UE (nel seguito "GDPR") MARIO ROSSI (nel seguito "Titolare") con sede in BRESCIA (BS), VIA DEL LAVORO, 20 – 25000, nella sua veste di "Titolare del trattamento", La informa che i Suoi dati personali raccolti ai fini della conclusione del contratto col Cliente e/o nell'ambito dell'esecuzione e/o della stipula dello stesso saranno trattati nel rispetto delle normativa citata, al fine di garantire i diritti, le libertà fondamentali, nonché la dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. La informiamo che qualora le attività a lei prestate prevedano il trattamento di dati personali di terzi nella sua titolarità sarà sua responsabilità assicurare di aver adempiuto a quanto previsto dalla normativa nei riguardi dei soggetti Interessati al fine di rendere legittimo il loro trattamento da parte nostra.

Origine, finalità, base giuridica e natura dei dati trattati

Il trattamento dei Suoi dati personali, da Lei direttamente forniti, è effettuato da MARIO ROSSI ai fini della conclusione del contratto col Cliente e/o nell'ambito dell'esecuzione e/o della stipula dello stesso. Altresì, è possibile il verificarsi di un trattamento di dati personali di terzi soggetti comunicati dal Cliente alla Società. Rispetto a tale ipotesi, il Cliente si pone come autonomo titolare del trattamento e si assume i conseguenti obblighi e responsabilità legali, manlevando la Società rispetto a ogni contestazione, pretesa e/o richiesta di risarcimento del danno da trattamento che dovesse pervenire alla Società da terzi interessati. Nel rispetto della normativa vigente in materia di protezione dei dati personali e senza necessità di uno specifico consenso da parte dell'Interessato, i Dati saranno archiviati, raccolti e trattati dalla Società per i seguenti fini:
a) adempimento a obblighi contrattuali, esecuzione e/o stipulazione del contratto col Cliente e/o gestione di eventuali misure precontrattuali;
b) assolvimento a eventuali obblighi normativi, alle disposizioni fiscali e tributarie derivanti dallo svolgimento dell'attività d'impresa e a obblighi connessi ad attività amministrativo-contabili;
c) invio, direttamente o tramite terzi fornitori di servizi di marketing e comunicazione, newsletter e comunicazioni con finalità di marketing diretto attraverso email, sms, mms, notifiche push, fax, posta cartacea, telefono con operatore, in relazione a prodotti erogati dalla altre società ai sensi dell'art. 130 c. 1 e 2 del D. lgs. 196/03 (nel seguito "Codice");
d) comunicazione dei Dati a società terze per l'invio di newsletter e comunicazioni con finalità di marketing attraverso email, sms, mms, notifiche push, fax, posta cartacea, telefono con operatore ai sensi dell'art. 130 c. 1 e 2 del Codice. Le basi giuridiche del trattamento per le finalità a) e b) sopra indicate sono gli artt. 6.1.b) e 6.1.c) del Regolamento. Il conferimento dei Dati per i suddetti fini è facoltativo, ma l'eventuale mancato conferimento dei Dati stessi e il rifiuto a fornirli comporterebbero l'impossibilità per la Società di eseguire e/o

stipulare il contratto ed erogare le prestazioni richieste dallo stesso. La base giuridica del trattamento di dati personali per le finalità c) e d) è l'art. 6.1.a) del GDPR in quanto i trattamenti sono basati sul consenso; si precisa che il Titolare può raccogliere un unico consenso per le finalità di marketing qui descritte, ai sensi del Provvedimento Generale del Garante per la protezione dei dati personali "Linee guida in materia di attività promozionale e contrasto allo spam" del 4 luglio 2013. Il conferimento del consenso all'utilizzo dei dati per finalità di marketing è facoltativo e qualora, l'interessato desiderasse opporsi al trattamento dei Dati per le finalità di marketing eseguito con i mezzi qui indicati, nonché revocare il consenso prestato; potrà in qualunque momento farlo senza alcuna conseguenza (se non per il fatto che non riceverà più comunicazioni di marketing) seguendo le indicazioni presenti alla sezione dei "Diritti dell'Interessato" della presente Informativa. Si ricorda infine che per i trattamenti effettuati ai fini di invio diretto di proprio materiale pubblicitario o di propria vendita diretta o per il compimento di proprie ricerche di mercato o di comunicazioni commerciali in relazione a prodotti o servizi analoghi a quelli utilizzati dal Cliente, la Società può utilizzare gli indirizzi di posta elettronica o anagrafici ai sensi e nei limiti consentiti dall'art. 130, comma 4 del Codice e dal provvedimento dell'Autorità Garante per la protezione dei dati personali del 19 giugno 2008 anche in assenza di consenso esplicito. La base giuridica del trattamento dei dati per tale finalità è l'art. 6, comma 1, lett. f) del GDPR, ferma restando la possibilità di opporsi a tale trattamento in ogni momento, seguendo le indicazioni presenti alla sezione dei "Diritti dell'Interessato" della presente Informativa.

Comunicazione

I dati potranno essere comunicati a soggetti terzi nominati responsabili del trattamento ai sensi dell'articolo 28 del GDPR e in particolare a istituti bancari, a società attive nel campo assicurativo, a fornitori di servizi strettamente necessari allo svolgimento dell'attività d'impresa, ovvero a consulenti dell'azienda, ove ciò si riveli necessario per ragioni fiscali, amministrative, contrattuali o per esigenze tutelate dalle vigenti normative. I Suoi dati personali, ovvero i dati personali di terzi nella sua titolarità, potranno altresì essere comunicati a società esterne, individuate di volta in volta, cui MARIO ROSSI affidi l'esecuzione di obblighi derivanti dall'incarico ricevuto alle quali saranno trasmessi i soli dati necessari alle attività loro richieste. Tutti i dipendenti, consulenti, interinali e/o ogni altra "persona fisica" che svolgono la propria attività sulla base delle istruzioni ricevute da MARIO ROSSI , ai sensi dell'art. 29 del GDPR, sono nominati "Incaricati del trattamento" (nel seguito anche "Incaricati"). Agli Incaricati o ai Responsabili, eventualmente designati, MARIO ROSSI impartisce adeguate istruzioni operative, con particolare riferimento all'adozione ed al rispetto delle misure di sicurezza, al fine di poter garantire la riservatezza e la sicurezza dei dati. Proprio in riferimento agli aspetti di protezione dei dati personali il Cliente è invitato, ai sensi dell'art. 33 del GDPR a segnalare a MARIO ROSSI eventuali circostanze o eventi dai quali possa discendere una potenziale "violazione dei dati personali (data breach)" al fine di consentire una immediata valutazione e l'adozione di eventuali azioni volte a contrastare tale evento inviando una comunicazione a MARIO ROSSI ai recapiti nel seguito indicati. I Dati non saranno diffusi. Resta fermo l'obbligo di MARIO ROSSI di comunicare i dati ad Autorità Pubbliche su specifica richiesta.

Trasferimento all'estero

Il trasferimento all'estero dei Suoi dati personali può avvenire qualora risulti necessario per la gestione dell'incarico ricevuto. Per il trattamento delle informazioni e dei dati che saranno eventualmente comunicati a questi soggetti saranno richiesti gli equivalenti livelli di protezione adottati per il trattamento dei dati personali dei propri dipendenti. In ogni caso saranno comunicati i soli dati necessari al perseguimento degli scopi previsti e saranno applicati gli strumenti normativi previsti dal Capo V del GDPR.

Modalità, logiche del trattamento e tempi di conservazione

I Suoi dati sono raccolti e registrati in modo lecito e secondo correttezza per le finalità sopra indicate nel rispetto dei principi e delle prescrizioni di cui all'art. 5 c 1 del GDPR. Il trattamento dei dati personali avviene mediante strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità stesse e, comunque, in modo da garantirne la sicurezza e la riservatezza. I Dati personali verranno trattati da MARIO ROSSI per tutta la durata dell'incarico ed anche successivamente per far valere o tutelare i propri diritti ovvero per finalità amministrative e/o per dare esecuzione ad obblighi derivanti dal quadro regolamentare e normativo pro tempore applicabile e nel rispetto degli specifici obblighi di legge sulla conservazione dei dati.

Diritti dell'Interessato

In conformità, nei limiti ed alle condizioni previste dalla normativa in materia di protezione dati personali riguardo l'esercizio dei diritti degli Interessati 1 per quanto concerne i trattamenti oggetto della presente Informativa, in qualità di Interessato Lei ha il diritto di chiedere conferma che sia o meno in corso un trattamento di suoi dati personali, accedere ai dati personali che La riguardano ed in relazione ad essi ha il diritto di richiederne la rettifica, la cancellazione, la notifica delle rettifiche e delle cancellazioni ai coloro i quali i dati sono stati eventualmente trasmessi dalla nostra Organizzazione, la limitazione del trattamento nelle ipotesi previste dalla norma, la portabilità dei dati personali - da Lei forniti - nei casi indicati dalla norma, di opporsi al trattamento dei suoi dati e, specificamente, ha il diritto di opporsi a decisioni che lo riguardano se basate unicamente su trattamenti automatizzati dei suoi dati, profilazione inclusa. Nel caso in cui ritenga che i trattamenti che La riguardano violino le norme del GDPR, ha diritto a proporre reclamo al Garante ai sensi dell'art. 77 del GDPR. Se intende richiedere ulteriori informazioni sul trattamento dei Suoi dati personali o per l'eventuale esercizio dei Suoi diritti, potrà rivolgersi per iscritto a Mario Rossi (mario.rossi@pec.it).

Titolare del Trattamento

Titolare del trattamento, ai sensi dell'art. 4 del GDPR, è:
MARIO ROSSI ,
VIA DEL LAVORO, 20 – 25000 BRESCIA (BS)
P.IVA: 23168454869
Tel.030 1234567
Email: m.rossi@pec.it

Il riferimento, all'interno dell'informativa, all'art. 14, definisce il caso in cui i dati provengano da fonti terze. In alcuni casi potrebbe rendersi necessaria la redazione di un'informativa specifica per quei casi specifici. Ricordiamo, inoltre, che nel caso in cui i dati provengano da fonti diverse dal titolare dei trattamenti, sarà necessario far pervenire l'informativa ed ottenere il consenso, quando necessario, al trattamento dei dati nel più breve tempo possibile e comunque non oltre 30 giorni.

9.b) Consensi privacy

Come già espresso precedentemente (vedi lo "Step 6"), il *consenso privacy* è obbligatorio in alcuni contesti (trattamento di dati particolari e/o per finalità non direttamente collegate all'esecuzione del contratto o di leggi) nei quali lo si deve definire come base giuridica per il trattamento di alcuni dati.

Il consenso può essere raccolto su supporto cartaceo; elettronico o via mail; telefonicamente con registrazione del messaggio, dopo l'esposizione vocale sintetica dell'informativa e via web, con l'utilizzo di "flag".

Il consenso privacy va richiesto dopo aver messo a disposizione l'informativa e prima di effettuare il trattamento di dati personali.

I consensi vanno conservati e devono restare a disposizione per eventuali verifiche. Il consenso deve essere rinnovato se, una volta scaduto il tempo di conservazione dei dati, si dovesse rendere necessaria una proroga al trattamento.

Non è necessario rinnovare il consenso se il dato è soggetto a conservazione di legge (10 anni) a fini fiscali. Sarà comunque obbligatorio, conservare tali dati in una zona protetta e non soggetta al trattamento richiesto dall'operatività quotidiana.

Di seguito, un esempio di consenso clienti:

MARIO ROSSI
VIA DEL LAVORO, 20 25000 BRESCIA (BS)
P. IVA 23168454869

ESPRESSIONE CONSENSO

A) DA PARTE DI PERSONA FISICA:

Il sottoscritto Sig. _____ prende atto della informativa resa ai sensi degli artt. 13 e 14 del Regolamento 2016/679/UE e accorda liberamente e volontariamente, ove richiesto, il consenso per le finalità indicate a che i propri dati personali possano essere trattati ed essere oggetto di comunicazioni ai soggetti per gli adempimenti connessi all'incarico conferito.
DATA _____/_____/_____ FIRMA _____

B) DA PARTE DI PERSONA GIURIDICA

L'Azienda _____, nella persona del legale rappresentante Sig. _____, in qualità di _____, prende atto della informativa resa ai sensi degli artt. 13 e 14 del Regolamento 2016/679/UE e accorda liberamente e volontariamente, ove richiesto, il consenso per le finalità indicate a che i propri dati personali dei quali l'Azienda è Titolare possano essere trattati ed essere oggetto di comunicazioni ai soggetti per gli adempimenti connessi all'incarico conferito, manlevando Organizzazione da ogni onere e responsabilità derivante dai previsti trattamenti.
DATA ____/_____/_____ FIRMA _____

C) CONSENSO PER MARKETING DIRETTO DELLA "RAGIONE SOCIALE"

Il sottoscritto Sig. _____ prende atto della informativa resa ai sensi degli artt. 13 e 14 del Regolamento 2016/679/UE e accorda liberamente e volontariamente, ove richiesto, il consenso per le finalità indicate al punto c) che i propri dati personali possano essere trattati ed essere oggetto di comunicazioni ai soggetti per gli adempimenti connessi all'incarico conferito.
DATA _____/_____/_____ FIRMA _____
\
E) CONSENSO PER MARKETING DIRETTO "TERZE PARTI"

Il sottoscritto Sig. _____ prende atto della informativa resa ai sensi degli artt. 13 e 14 del Regolamento 2016/679/UE e accorda liberamente e volontariamente, ove richiesto, il consenso per le finalità indicate al punto d) che i propri dati personali possano essere trattati ed essere oggetto di comunicazioni ai soggetti per gli adempimenti connessi all'incarico conferito.
DATA _____/_____/_____ FIRMA _____

Step 10. La formazione obbligatoria e l'audit periodico.

Uno specifico articolo del regolamento europeo, l'art. 29, prevede che chiunque tratti dati personali, debba ricevere un'adeguata formazione specifica sui principi generali della normativa.
In realtà, il processo di formazione deve comprendere i seguenti temi:

- i principi generali del regolamento europeo e della sua applicazione nello stato nel quale si opera;
- le buone pratiche relative alla sicurezza informatica;
- le procedure e i processi applicati all'interno della propria organizzazione che coinvolgono il trattamento di dati personali;
- i propri diritti e doveri rispetto al trattamento dei dati personali e i limiti nel trattamento degli stessi, in relazione alle proprie mansioni in azienda;
- le regole aziendali e le istruzioni per il corretto utilizzo dei dispositivi di trattamento dei dati in azienda.

Parliamo di un "processo" di formazione, in quanto caratterizzato da una dinamicità nel tempo dei contenuti. Ciò presuppone l'applicazione della pratica di "formazione continua" e della conseguente programmazione, almeno annuale, di sessioni formative specifiche.
In caso di ispezione, a campione o successiva ad un evento di data breach, non sarà sufficiente mostrare degli attestati ma dimostrare che le persone, che, per il ruolo svolto, gestiscono dei dati personali, abbiano realmente appreso tutti i concetti relativi alla loro tutela, protezione e difesa.
Il processo di formazione è parte integrante delle misure organizzative adeguate da applicare, così come vengono intese all'interno del testo del GDPR.

Il titolare dei trattamenti, cioè l'impresa che gestisce i dati, dovrà preoccuparsi di adeguare dal punto di vista anche formativo tutti gli autorizzati al trattamento al suo interno, cioè tutti i dipendenti e collaboratori, nonché amministratori e soci che, per le mansioni che svolgono, trattano dati personali.

E' consigliabile, per la formazione, rivolgersi a enti o aziende di comprovata esperienza e affidabilità.

Abbiamo inserito nello stesso step, formazione e audit (revisione e aggiornamento periodico dell'adeguamento) in quanto è possibile far coincidere l'appuntamento periodico, tipicamente annuale, con chi può effettuare queste due attività.

Il GDPR è stato pensato proprio per una realtà che, grazie allo sviluppo tecnologico nel campo della comunicazione e dell'elaborazione di dati, presenta oggi un grado di dinamicità mai riscontrato in passato. Ma a cambiare non è solamente l'ambiente circostante, ma anche la propria impresa per via del turnover fisiologico del personale, per l'implementazione dei nuovi processi o per il cambio dell'infrastruttura informatica o di quella organizzativa. Se a questo, aggiungiamo provvedimenti legislativi e l'emissione di nuove linee guida da parte dell'autorità del Garante, diventa indispensabile concepire l'adeguamento alla privacy come un processo in continuo divenire.

Nel momento della realizzazione di questo manuale è attuale la problematica relativa ai provvedimenti di contrasto all'epidemia del virus Covid 19, situazione che prospetta per il futuro il trattamento di dati relativi la situazione sanitaria dei dipendenti in modo particolare e impensabile rispetto al passato. Ad esempio, è attuale, in alcune realtà, l'obbligo di misurazione della temperatura corporea all'ingresso dell'azienda, operazione che va compiuta sempre nel rispetto di alcune regole di base e dopo aver effettuato un'accurata analisi di impatto privacy.

E' consigliabile quindi restare costantemente aggiornati sugli sviluppi della normativa, delle tecnologie e delle applicazioni tecnologiche, così da potersi muovere agevolmente nel labirinto delle normative e nel rispetto dei principi fondamentali delle libertà e dei diritti fondamentali di ognuno, consci dei vantaggi, in termini di reputazione, di sicurezza e di inattaccabilità in caso di controversie.

Ricapitolando:

i documenti di base previsti sono:

- analisi dei rischi – analisi di impatto;
- registro dei trattamenti;
- atti di incarico e nomina (autorizzati al trattamento; responsabili esterni);
- informative e consensi.

Formazione obbligatoria per chi tratta i dati.

2 - I soggetti e ruoli

Nei prossimi paragrafi vedremo, per ogni tipologia di soggetto interessato al trattamento di dati personali, le caratteristiche e le tematiche che lo riguardano in relazione alla normativa e alle buone pratiche da applicare in azienda.

2- a I dipendenti

Come accennato nella parte introduttiva, i dati personali trattati nell'ambito aziendale riguardano molte diverse tipologie di soggetti. Se pensiamo ad aziende che trattano affari con altri soggetti giuridici o anche imprese che, pur vendendo a privati, si limitano ad azioni commerciali senza trattamento di dati (pensiamo a chi vende al minuto), sicuramente, la gestione della privacy e della protezione dei dati personali riguarda in particolare i propri dipendenti (essi diventano, rispetto all'azienda, "soggetti interessati al trattamento"). Una visita di controllo da parte dell'Ispettorato del Lavoro potrebbe comprendere un'ispezione specifica della documentazione e delle misure idonee intraprese per la salvaguardia dei dati dei dipendenti e collaboratori.

I dati trattati nell'ambito del rapporto di lavoro sono sicuramente molto sensibili ma non richiedono alcun consenso firmato da parte del lavoratore, in quanto la base giuridica che rende lecito il loro trattamento è rappresentata dal contratto di lavoro. Resta comunque necessario mettere a disposizione le informative sui trattamenti previsti. Le informative sul trattamento che riguardano i dipendenti sono le seguenti:

- informativa per il trattamento dei dati di base gestiti per via del rapporto di collaborazione;

- informativa per il trattamento dell'immagine a scopo di marketing (se acconsentono all'utilizzo);

- informativa per i candidati da selezionare per l'assunzione;

- informativa per impianto di videosorveglianza;

- informativa per l'impianto di geo localizzazione veicolare.

All'interno del "registro dei trattamenti" (vedi paragrafo 1-e, step 8) vanno inseriti i nomi dei dipendenti coinvolti negli specifici trattamenti di dati. Gli stessi dipendenti riceveranno l'atto di nomina per l'incarico di "autorizzazione al trattamento" (vedi paragrafo 1 e, step 3) e la formazione obbligatoria (vedi paragrafo 1 e, step 10).

Il regolamento europeo auspica per l'implementazione in azienda di *policy* (regolamenti condivisi) che regolano l'utilizzo dei dispositivi aziendali (pc, smartphone, account di mail, etc.). Consigliamo fortemente l'adozione delle policy, non solo per dimostrare, in caso di controllo, di aver attuato tutte le misure organizzative idonee, ma anche per tutelare l'azienda in caso di condotta scorretta da parte del lavoratore.
La policy deve prevedere l'utilizzo esclusivo a scopo professionale dei dispositivi aziendali e la possibilità di gestire in modo consono la casella di posta elettronica in caso di assenza del lavoratore per ferie o malattia o in caso di interruzione del rapporto di lavoro. In questi casi, infatti, è necessario seguire una procedura ben precisa: deve essere nominata una persona diversa dal titolare o dal diretto responsabile (un collega o l'amministratore di sistema) che ha il compito di estrarre dalla casella di posta del dipendente assente solo i messaggi strettamente necessari all'attività lavorativa. Deve essere poi steso un rapporto che certifichi questa attività e informato il dipendente interessato. Tutto ciò però deve essere previsto e inserito nella policy.
Ricordiamo che i dispositivi, come i pc, i telefoni, etc., sono di proprietà dell'azienda, ma il contenuto, in particolare quello dell'account di posta, è di pertinenza del lavoratore e accedervi può significare compiere un abuso. Ci sono già molte sentenze emesse a tal proposito dagli organi giudiziari.

2- b I clienti

E' fondamentale distinguere i clienti "soggetto giuridico" dai clienti "persona fisica". Ricordiamo che il GDPR prevede l'applicazione della normativa a quest'ultima categoria. Ovviamente, è vero che anche i soggetti giuridici sono rappresentati da persone fisiche, ma dobbiamo preoccuparci solo dei dati personali.

I casi in cui è necessario raccogliere il consenso esplicito, sono generalmente i seguenti:

- utilizzo di numeri di cellulare e mail personali;

- utilizzo dei dati a scopo di marketing (newsletter, offerte, profilazioni, carte fedeltà, etc.);

- trattamento di dati particolari (sensibili), come ad esempio dati di reddito, dati sanitari, dati giudiziari, etc.;

Non è necessario far firmare consensi se i dati trattati sono esclusivamente quelli indispensabili alla singola fornitura (dati fiscali; indirizzo; recapiti). In questo caso, la base giuridica è l'esecuzione del contratto o la legge nazionale, nel caso di dati fiscali. Se però viene utilizzato un recapito, magari la mail, per inviare promozioni e offerte, serve il consenso, anche se il cliente è un soggetto giuridico. E' l'unico caso in cui si incrociano gli adempimenti sulle due tipologie di soggetti. Ricordiamo che una ditta individuale, per quanto possessore di partita iva, è considerato soggetto privato ai fini privacy.

L'informativa, al di là della necessità o meno di firma di un consenso, dovrà sempre essere presente.

2- c Gli agenti e i rappresentanti di commercio

La struttura di un'agenzia può comprendere la sola figura dell'agente o un team composto da vari agenti e collaboratori. In tutti i casi, l'organizzazione deve effettuare gli adeguamenti, anche se la struttura è quella di "micro impresa".

Di seguito, le principali particolarità in tema di normativa:

l'agente o gli agenti, a seconda di come sono organizzati (competenze interne), assumono il ruolo di:

- titolari del trattamento nei confronti dei loro collaboratori/dipendenti; fornitori; visitatori; (se sono più agenti associati, potrebbero assumere il ruolo di contitolarità dei trattamenti);

- responsabili esterni dei trattamenti nei confronti della mandante e dei clienti. Questo perché l'attività di trattamento dati effettuata verso i clienti è determinata dalla volontà della casa mandante, cioè, l'agente tratta i dati per finalità determinate da quest'ultima.

Avendo quindi il "doppio ruolo" (titolari e responsabili esterni del trattamento) gli agenti dovranno redigere due registri dei trattamenti, uno per ruolo. I casi di contitolarità sono da normare con atti giuridici ad hoc, esattamente come i casi di responsabilità esterna.

Potrebbero verificarsi dei casi in cui gli agenti sono nominabili semplicemente come "autorizzati al trattamento" dai titolari, cioè dalle case mandanti. Generalmente, ciò avviene quando l'attività dell'agente viene svolta a stretto contatto con la mandante, magari utilizzando, come supporto, gli uffici e i supporti informatici di quest'ultima. In questo caso, la responsabilità di eventuali violazioni sui dati è totalmente della mandante, in quanto gli autorizzati rappresentano "il lungo braccio dei titolari".

2- d I visitatori e i fornitori

Tracciare la presenza in azienda dei visitatori è un legittimo interesse del titolare del trattamento oltre che un dovere per le normative riguardanti la sicurezza aziendale. Non sono previsti consensi da richiedere a meno che non vengano effettuati trattamenti particolari di dati.

Non è consentito trattenere e fotocopiare documenti di identità o raccogliere recapiti privati.

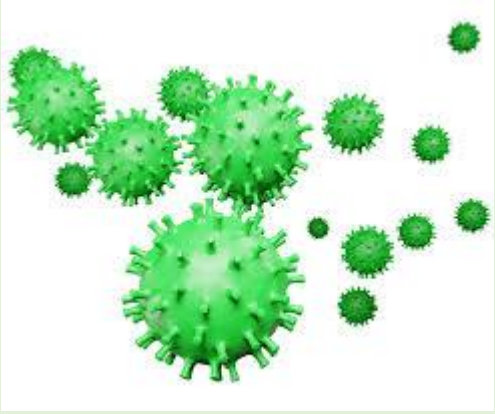
E' possibile e, anzi, consigliato, richiedere il modulo "Unilav" alle aziende che inviano, presso l'azienda titolare dei trattamenti, maestranze per compiere lavori di manutenzione. Questo per dimostrare, in caso di ispezione da parte dell'Ispettorato del Lavoro, che quei lavoratori sono regolarmente assunti dall'impresa incaricata dei lavori.

Come per i casi riguardanti gli altri soggetti e gli altri trattamenti, dovrà sempre essere presente l'informativa specifica.

2- e I visitatori del sito web

Il sito web deve consentire l'accesso all'informativa privacy riservata a chi accede e a chi compila sezioni di richiesta di informazioni. L'informativa riguarda principalmente la gestione dei dati forniti dal visitatore (nel momento in cui compila dei form o accede ad un sistema di e-commerce) e i *cookies* (applicazioni software di tracciamento e analisi) presenti nel sito. L'utente deve poter scegliere se acconsentire o meno all'installazione dei cookies nel suo dispositivo. Gli unici cookies consentiti per "default" sono che consentono la corretta visualizzazione del sito. Ricordiamo che il numero "IP" (numero che identifica il dispositivo dell'utente che si connette) è considerato "dato personale".

3 - La privacy e il Covid – 19



Al momento della stesura del presente manuale, sono in vigore le disposizioni ministeriali finalizzate al contenimento della pandemia nei pubblici esercizi e negli ambienti di lavoro.

Riassumiamo, di seguito, le principali misure prescritte e le relative modalità di applicazione in ambito privacy:

a) misurazione della temperatura all'ingresso della propria attività:

il dato della temperatura non deve mai essere trascritto o memorizzato, tranne che nel caso della verifica effettuata a personale dipendente risultato superiore a 37,5°C. In questo caso è necessario mantenere il dato, utilizzando tutte le misure idonee per la sua tutela e protezione, a dimostrazione del divieto di frequentazione dell'ambiente di lavoro. E' prevista la comunicazione del dato esclusivamente agli organi sanitari competenti; la conservazione del dato è ammessa fino alla completa guarigione del collaboratore e, se esiste una valida ragione, fino alla fine dell'emergenza Covid.

Il titolare dell'attività o il dirigente in loco, può autorizzare una o più persone dell'azienda all'effettuazione del trattamento.

Se il trattamento viene effettuato tramite termoscanner automatici è necessario redigere la valutazione di impatto privacy (art. 35 del GDPR);

b) autocertificazioni per esclusione di contatti a rischio:

utilizzate da datori di lavoro per i propri dipendenti e da alcune categorie che prevedono contatti prolungati e ripetuti, le autocertificazioni devono essere gestite dal titolare o da personale autorizzato e vanno conservate per max 14 giorni o fino al termine dell'emergenza (dipendenti) in luoghi sicuri e protetti che ne garantiscano l'inviolabilità e la riservatezza;

c) elenco avventori:

l'adempimento è previsto per alcune categorie, come ad esempio, i ristoratori. L'elenco deve contenere: data, nome, cognome e numero di telefono. La conservazione del documento non può superare i 14 giorni e, come per le autocertificazioni, deve essere conservato in un luogo sicuro e l'accesso al documento deve essere limitato agli autorizzati;

c) informativa:

l'informativa deve essere specifica e riportare tutte le attività anti Covid: deve riportare tutti i dati previsti (vedi paragrafo relativo alle informative). La base giuridica da indicare è il decreto del Consiglio dei Ministri con le disposizioni specifiche. Si può, vista la variabilità indicare in modo più generico. Le informative vanno apposte ben in vista, in prossimità delle rilevazioni;

e) consensi:

tutti i trattamenti elencati non necessitano di consenso, dato che la base giuridica, come già detto, è la disposizione del decreto del Consiglio del Ministri;

f) altra documentazione privacy:

i trattamenti devono essere riportati nel registro dei trattamenti e nelle analisi del rischio privacy; devono essere redatte le autorizzazioni per il personale designato ai trattamenti e le strumentazioni e i dispositivi impiegati vanno inseriti nell'elenco degli "asset di trattamento".

4 - La videosorveglianza e la geo localizzazione

4- a La videosorveglianza

Mai come in questi anni il tema della videosorveglianza risulta attuale e, in alcuni casi, piuttosto controverso, in particolare se utilizzato a scopo di controllo della popolazione,

magari abbinato ad un sistema di riconoscimento facciale, da parte di governi autoritari, o come "captatore" di espressioni dell'acquirente a scopo di marketing.
Il discorso è molto ampio e sarebbero necessari svariati testi per affrontare il tema in tutte le sue sfaccettature.

In questo manuale ci limiteremo a trattare il tema della videosorveglianza nei suoi utilizzi più comuni, da parte di entità private per le finalità "standard", già previste anche dall'Ispettorato del lavoro, quando coinvolgono collaboratori aziendali. Parliamo quindi delle seguenti finalità:

1) **Tutela e sicurezza del patrimonio aziendale.**

E' piuttosto intuitivo: si installa un sistema di rilevazione video per evitare furti e danneggiamenti del proprio patrimonio.

2) **Sicurezza sul lavoro.**

Si installano telecamere per monitorare attività lavorative piuttosto pericolose, che implicano l'utilizzo di macchinari particolari o che vengono svolte in ambienti rischiosi.

3) **Organizzazione dell'attività lavorativa.**

Pensiamo al monitoraggio della sala di un ristorante, attuata per verificare la presenza di avventori o le telecamere installate

Sono vietate attività di controllo a distanza dei lavoratori o riprese effettuate all'insaputa dei soggetti interessati.
Non sono ammesse telecamere finte a scopo deterrente in ambienti con dipendenti.

Verifichiamo di seguito le caratteristiche principali del trattamento di videosorveglianza e gli adempimenti previsti (per la redazione dei documenti e le nomine, vedi il capitolo "Adeguamento della propria impresa al GDPR"):

1) Base giuridica.

Nei casi di tutela del patrimonio e dell'organizzazione dell'attività, la base giuridica da utilizzare è generalmente quella del *legittimo* del titolare del trattamento;

nel caso della sicurezza sul lavoro, conviene verificare se esistono, nei casi specifici, delle normative nazionali che prevedono il controllo di tali attività. Un esempio di legge nazionale (della pubblica sicurezza), da utilizzare come base giuridica, è il caso dell'installazione nelle sale da gioco: in questo caso l'installazione è obbligatoria per svolgere l'attività.

Non è prevista la base giuridica del consenso. Ricordiamo poi che il consenso, se richiesto ai propri dipendenti, in caso di controversia

giudiziaria, verrebbe rigettato dal giudice, in quanto, il dipendente è ritenuto in posizione di assoggettamento rispetto al datore.

2) Diritti previsti per i soggetti interessati.

I diritti applicabili sono quelli dell'oblio, della cancellazione, dell'opposizione, dell'accesso e della trasparenza.

3) Nomine e designazioni.

E' necessario istruire e nominare "autorizzato al trattamento" chi si occuperà di gestire l'impianto; se la gestione viene effettuata da una società esterna o se le immagini vengono inviate ad una società di vigilanza, sarà necessario nominare tali soggetti come "responsabili esterni del trattamento".

4) Documenti GDPR.

E' necessario implementare la documentazione privacy di base con i seguenti documenti:

a) Valutazione di impatto privacy. Deve essere effettuata, in quanto il trattamento in questione rappresenta un trattamento automatizzato di dati biometrici (immagini);
b) Inserimento delle descrizioni dei dispositivi impiegati all'interno dell'"elenco degli asset";
c) Inserimento del trattamento, dei soggetti implicati, delle misure di sicurezza e di tutte le informazioni previste nel "registro dei trattamenti";
d) Redazione dell'informativa completa specifica per il trattamento. Metterla a disposizione per chi la dovesse richiedere;
e) Applicazione dei cartelli di avviso di videosorveglianza (informativa sintetica) appena prima del raggio d'azione delle telecamere, in luogo ben visibile, ad un'altezza di circa mt. 1,70.

5) Misure tecniche e organizzative da applicare.

Il dispositivo di videoregistrazione, nonché le riprese, devono essere accessibili: solo da personale designato e formato; vincolato da utilizzo di password e sistema di log management; protetto da potenziali effrazioni; consultato solo se presente reale motivazione. Le linee guida suggeriscono la crittografia dei dati e la conservazione dei registri dei log, che certificano la visione delle riprese, per almeno 6 mesi, se queste vengono effettuate da remoto, via smartphone o tablet.

6) Tempi di conservazione.

Le immagini possono essere conservate, generalmente per 24/48 ore (giorno festivo), ma, per esigenze particolari, fino a 7 giorni. Per periodi più lunghi è necessario fornire valide motivazioni. Recentemente il Garante ha tolto il vincolo stringente dei tempi di conservazione, ma se il titolare/responsabile del trattamento non è in grado di motivarne adeguatamente la scelta, il rischio di sanzioni è elevato.

7) Autorizzazione sindacale o dell'Ispettorato del lavoro (in caso di presenza di dipendenti/collaboratori)

Se la videosorveglianza riprende zone di competenza dell'azienda (interni; cortili; zona carico/scarico; etc.) si rende necessaria l'autorizzazione richiesta alla rappresentanza sindacale interna. Se non presente o se non si dovesse trovare un accordo, l'ente al quale rivolgersi è l'ufficio territoriale del Dipartimento del Lavoro.

Tutti gli adempimenti descritti devono essere svolti **indipendentemente** dalla presenza del dispositivo di videoregistrazione e dagli orari di funzionamento dell'impianto.

4- b La geo localizzazione

I dispositivi di geo localizzazione, grazie all'estesa rete di satelliti sviluppata negli ultimi decenni, rappresentano oggi alcuni tra gli strumenti più utilizzati per una serie infinita di scopi, sia privati che aziendali: navigazione stradale; tracciamento per finalità assicurative; localizzazione per organizzazione logistica; etc**.**

In questa sede ci occuperemo della gestione delle problematiche e adempimenti relativi alla privacy, in caso di installazione dei dispositivi localizzatori gps sulle auto o sui furgoni aziendali, condotti da personale dipendente o con rapporto di collaborazione, per le finalità di: assistenza; organizzazione logistica e sicurezza. Resta inteso il divieto, come per tutti i dispositivi di rilevazione, del controllo a distanza del collaboratore.

Vediamo quali sono le disposizioni e i documenti necessari affinché il trattamento sia lecito.

Per la redazione dei documenti e delle nomine elencate di seguito, si invita a consultare il capitolo "Adeguamento della propria impresa al GDPR (per tutte le imprese)

Caratteristiche tecniche e gestione dell'impianto:

1) il localizzatore deve essere momentaneamente disattivabile per consentire al lavoratore di tutelare la propria privacy nei momenti di pausa dal lavoro;

2) il tracciamento deve essere dettagliato il meno possibile, in relazione alla finalità. Per esempio, potrebbe non esserci la necessità di tracciare la posizione del veicolo ogni 20 secondi, se la finalità è quella di organizzare gli appuntamenti per un'assistenza tecnica. Potrebbe essere sufficiente interrogare il sistema ogni 15/20 minuti. Purtroppo non esistono indicazioni dettagliate da parte del Garante. Tuttavia, in passato sono state comminate delle sanzioni a causa di un tracciamento troppo frequente, con la motivazione di un utilizzo "oltre misura" dei dati necessari;

3) il sistema deve indicare, tramite un'icona o un segnale, quando è attivo;

4) la localizzazione deve essere oscurata, dopo un periodo di inattività, sul monitor di chi è addetto al controllo della posizione del veicolo;

5) i report dei tragitti, consegnati dall'azienda ai clienti, non devono consentire l'identificazione dei dipendenti;

6) predisporre periodiche verifiche tecniche per valutare l'affidabilità e il buon funzionamento dell'impianto;

7) i tempi di conservazione dei dati dei tragitti devono essere ridotti al minimo indispensabile;

8) il personale dell'azienda addetto al trattamento dei dati di localizzazione devono essere formati sui principi del GDPR e devono essere nominati come designati al trattamento;

9) se il servizio viene svolto da una società esterna quest'ultima deve essere nominata come responsabile esterno del trattamento, come pure il fornitore del software di localizzazione.

Autorizzazioni e documenti:

1) richiesta di autorizzazione alla rappresentanza interna all'azienda; se non presente o se non si giunge ad un accordo, richiederla alla direzione territoriale dell'Ispettorato del lavoro, esattamente come per gli impianti di videosorveglianza;

2) redazione della *valutazione di impatto privacy (dpia)*;

3) inserimento della descrizione dei dispositivi impiegati nell'elenco degli *asset di trattamento dati* aziendali;

4) inserimento del trattamento all'interno del registro dei trattamenti con tutte le informazioni previste;

5) redazione dell'informativa specifica o inserimento di tutte le caratteristiche previste dal trattamento all'interno *dell'informativa dipendenti* (informare i dipendenti del nuovo trattamento e della nuova informativa).

Basi giuridiche del trattamento:

il trattamento non prevede, generalmente, la base giuridica del *consenso.*
Bisogna analizzare le reali motivazioni dell'esigenza della localizzazione, normalmente le motivazioni e, di conseguenza, le corrispondenti basi giuridiche sono:

- sicurezza sul lavoro (aeromobili e natanti);

- esecuzione del contratto (società di taxi; società di consegna veloce di pasti a domicilio);

- legittimo interesse del titolare (aziende di trasporti; società di assistenza tecnica; società di approvvigionamento e logistica; etc.);

- in casi eccezionali, situazioni di emergenza o salvaguardia della vita (squadre di emergenza alpina; mezzi di soccorso; etc.);

- leggi nazionali (portavalori).

Se il servizio viene svolto da una società esterna specializzata, è necessario chiedere l'applicazione delle misure tecniche e organizzative precedentemente descritte.

5 - La sicurezza informatica

Potrebbe sembrare inutile ribadirlo ma l'importanza della sicurezza informatica, in un'epoca nella quale i dati vengono trattati attraverso l'utilizzo in rete di pc, smartphone e server, è fondamentale. Eppure il nostro paese dedica ancora oggi troppe poche risorse a quegli strumenti, che vengono definiti dal Gdpr "idonee misure tecniche e organizzative", indispensabili per la protezione delle informazioni e dei dati personali.

Il vecchio ordinamento privacy comprendeva l'"allegato B" che riportava tutti i requisiti minimi che i dispositivi informatici dovevano rispettare. I criteri di base e le buone pratiche restano sempre valide anche se è necessario mantenersi costantemente aggiornati rispetto alle nuove tecnologie e alle nuove possibili cyber – minacce.

Alcune istruzioni di base potranno sembrare scontate a molti, ma è sempre bene ribadirle.

Pc, server e smartphone, devono essere configurati con software aggiornati e password. La password deve essere impostata sia per l'accensione del dispositivo, sia per ogni applicazione e deve consentire l'accesso ai dati sulla base di profili utente, distinti sulla base dei ruoli aziendali.

La password deve avere almeno 8 caratteri alfanumerici, contenere maiuscole, minuscole e caratteri speciali. La sua sostituzione deve avvenire almeno ogni tre mesi e non deve essere divulgata o conservata in prossimità del dispositivo. Bisogna evitare di utilizzare la stessa password per più dispositivi e applicazioni.

E' indispensabile prevedere l'utilizzo di sistemi antivirus su tutti i dispositivi aziendali. L'antivirus deve prevedere almeno le seguenti funzionalità:

- verifica periodica di tutto il dispositivo;
- verifica dei file, prima del loro download e apertura e/o apertura in una "sandbox";
- verifica delle porte usb;
- verifica dei siti web in fase di navigazione;
- funzione di firewall;
- funzionalità anti ransomware;
- funzionalità antispyware.

Per migliorare la sicurezza e la funzionalità del pc è consigliabile effettuare frequenti "pulizie" e "ottimizzazioni" dei dischi, utilizzando le funzioni di pulizia, di ottimizzazione e di compattamento presenti in Windows o tramite apposite applicazioni.

Di seguito, alcune buone pratiche per aumentare la sicurezza dell'utilizzo del dispositivo:

- eliminare quotidianamente eventuali cookies e cronologie;
- non memorizzare password e credenziali nei dispositivi;
- non navigare su siti web poco sicuri (verificare l'indirizzo: deve comparire nella stringa "https" e non solamente "http");
- impostare il browser e l'antivirus in modo che tutti i cookies vengano bloccati di default ed eventualmente sbloccati manualmente;
- evitare di scaricare file e applicazioni dal Web da indirizzi sconosciuti e/o per motivi che esulano da necessità di tipo professionale o se non autorizzati dal datore di lavoro;
- non utilizzare reti wifi gratuite e libere provenienti da fonti ignote;
- utilizzare solo programmi di posta elettronica professionali;
- non utilizzare programmi di messaggistica e social network, per uso privato, se non autorizzati e normati dal datore di lavoro;
- non utilizzare il dispositivo collegato a wifi e hot spot privati e a dispositivi di domotica.

In alcuni casi e, quando possibile, sarebbe bene non consentire l'utilizzo delle porte USB senza autorizzazione, per evitare l'inserimento di chiavette o hard disk non controllati, potenzialmente infetti e utilizzabili come supporti per copiare illecitamente file contenenti dati riservati.

Sarebbe bene dotare di antivirus anche lo smartphone e comunque evitare, su quest'ultimo, di memorizzare dati personali, salvo eventuali nominativi in rubrica.

Gli attacchi più probabili ad una rete informatica, da parte di malintenzionati, possono essere i seguenti:

- attacchi sintattici: installazione di software malevoli (virus, worm, trojan horses) che infettano i sistemi, diffondendosi anche su più dispositivi, generando danni, rallentamenti o trafugando dati;
- attacchi semantici: modifiche di dati o informazioni esistenti o diffusione di informazioni errate;
- intrusioni tramite la pratica "man in the middle", che consiste nell'intercettazione di comunicazioni tra due o più interlocutori;
- attacco Ddos (Distribuited Denial of Service): è un attacco diretto contro siti web; server o interi sistemi informatici, effettuato allo scopo di interrompere o rallentare molto un servizio, generando una grave disfunzione;
- ransomware: si tratta di un malware in grado di criptare il contenuto di un dispositivo o limitarne l'accesso. Per la decriptazione o lo sblocco del dispositivo, viene chiesto un riscatto, normalmente in criptovaluta.

A tutte queste potenziali minacce dobbiamo aggiungerne due, spesso poco considerate:

1) furto fisico di un dispositivo;
2) collaboratore infedele o non rispettoso delle regole di riservatezza e di utilizzo lecito dei dati.

I rischi connessi al primo caso, quello del furto fisico del dispositivo, a patto che nello stesso siano memorizzati dei dati, possono essere ridotti drasticamente o eliminati utilizzando, in primo luogo, una password complessa per l'apertura del pc, ed eventualmente un buon programma di crittografia dei dati che richieda una chiave di decriptazione complessa.
Per tenere invece "sotto controllo" il proprio patrimonio aziendale, evitando potenziali abusi da parte del collaboratore, è consigliabile prima di tutto definire un perimetro di consultazione dei dati, in base al ruolo svolto in azienda; sembra banale ricordarlo, ma, in molte imprese, in particolare se piccole e poco strutturate, l'accesso ai sistemi non è ben regolamentato e spesso tutti i dipendenti possono accedere a tutti i dati dell'azienda.
In secondo luogo, è bene implementare, nei database aziendali, un buon sistema di *log management*, cioè un'applicazione che tracci qualsiasi ingresso, esportazione, modifica o cancellazione dei dati contenuti. In questo modo, in caso di abusi, è più semplice risalire ai responsabili.

L'eliminazione dei dati personali dai propri sistemi, a seguito di richiesta esplicita dei soggetti interessati (diritto all'oblio) e/o per mancanza di una finalità di trattamento, una volta espletata la gestione commerciale e fiscale dell'esecuzione di un contratto, deve avvenire in modo definitivo. Per garantire ciò, sarà necessario, in caso di documentazione cartacea, utilizzare gli appositi strumenti di distruzione documentale; in caso di dato trattato con dispositivi informatici, procedere con l'eliminazione definitiva (in particolare quando si sta eliminando il dispositivo) utilizzando gli appositi software di cancellazione oppure con la distruzione fisica dell'hard disk; in caso di dato diffuso in rete, procedere con la deindicizzazione dai motori di ricerca e con l'eliminazione delle tracce presenti nel web sui portali nei quali i dati potrebbero essere confluiti.

6 - La gestione delle violazioni di dati personali.

Il *data breach,* definibile in italiano come “violazione di dati”, in realtà potrebbe ampliare la sua accezione comprendendo anche il significato di “incidente sui dati”. Questo perché non è detto che la perdita di riservatezza, integrità o disponibilità del dato derivi necessariamente da un illecito voluto. Alcuni data breach possono essere generati sicuramente da episodi di *hackeraggio informatico* o da furto di documenti cartacei o digitali, ma non sono da escludere black out delle reti; invii di posta elettronica ad errati destinatari o errori nella gestione dei sistemi informatici.

La normativa impone un iter ben preciso da seguire, nel caso in cui un evento del genere dovesse verificarsi.

La prima azione da compiere è riportare data, ora, descrizione sommaria dell’evento e azioni compiute successivamente su un *registro degli incidenti e delle violazioni* (si tratta di un semplice foglio o blocco di note, volendo anche digitale, da conservare in azienda);

successivamente, si effettua una valutazione, aiutandosi anche con l’analisi dei rischi, precedentemente redatta, dei rischi a cui sono sottoposti i soggetti interessati e le potenziali conseguenze. Facciamo due esempi pratici:

1) si subisce un furto di un pc; il pc non contiene dati personali oppure li contiene ma sono criptati. Rischio: basso; conseguenze per i soggetti interessati: nessuna;

2) si subisce un’intrusione informatica; i dati riguardano dati personali sensibili (documenti; buste paga; etc.). Rischio: alto; conseguenze per i soggetti interessati: potenziali truffe; diffusione e utilizzo illecito dei dati.

A questo punto, una volta individuati i rischi per i soggetti interessati, si procede nel seguente modo:

1) rischio basso di violazione di diritti e libertà fondamentali dell’individuo:

a) sul registro degli incidenti e delle violazioni si riportano i dati fondamentali del data breach e si procede per il ripristino della condizione precedente;

b) si segna sul registro il motivo per cui il rischio è stato definito basso;

2) rischio alto di violazione di diritti e libertà fondamentali dell’individuo:

a) entro 72 ore dall’evento (o da quando si è scoperto) si effettua una dettagliata comunicazione al Garante della privacy, nella quale si descrive nel dettaglio:

- tipologia dell’evento, data, ora;
- tipologia di dati violati, sommaria quantità di dati violati e sommaria quantità di soggetti coinvolti;
- potenziali conseguenze della violazione sui soggetti interessati;
- misure di tutela e protezione applicate ex-ante evento;
- misure da intraprendere ex-post evento sia per il ripristino della situazione precedente che per la tutela e la protezione futura;
- descrizione della modalità di informazione della violazione ai soggetti interessati.

b) nel più breve tempo possibile, informare i soggetti interessati dell’avvenuta violazione. La modalità di informazione può essere via missiva, posta elettronica, pubblicazione a mezzo stampa (se i soggetti sono estremamente numerosi).

Nel sito del Garante è possibile trovare la modulistica di riferimento per la compilazione della relazione anche se è possibile redigerla seguendo un modello proprio. L’importante è che siano riportate tutte le informazioni previste dal regolamento.

Conclusioni

Ci auguriamo che questo breve viaggio compiuto nei meandri di una materia piuttosto ostica, come quella della privacy e della protezione dei dati, sia stato utile per consentire di ottenere una visione generale di come deve essere affrontato il tema all'interno della azienda e di quali siano le tematiche e gli aspetti principali dell'argomento rispetto anche agli adempimenti da espletare.
Invitiamo tutti gli imprenditori che desiderino implementare il GDPR in azienda a fare molta attenzione a come vengono redatti i documenti e di utilizzare i sistemi di sicurezza dei dati più efficienti; ad informarsi attraverso il sito del Garante e attraverso letture più approfondite del regolamento. Gli esempi, i modelli e le soluzioni, riportate all'interno del manuale, sono puramente indicativi.
Nella realtà di un'impresa potrebbe essere necessario adottare soluzioni specifiche che necessitano di un'analisi e di una competenza approfondita. Inoltre, è necessario restare aggiornati sulle linee guida e sui chiarimenti pronunciati dal Garante; sulle sentenze pronunciate dalle procure; sulle indicazioni provenienti dall' EDPB (European Data Protection Board).

Il team di Kruzer e Hqc resta a disposizione per qualsiasi necessità legata al tema degli adeguamenti privacy.

Contatti

Per qualsiasi chiarimento, potete contattare i seguenti recapiti:

Kruzer

Tel.: 030 300083

E – mail: info@kruzer.it
Sito web: www.kruzer.it

Il team dei nostri consulenti, formato da avvocati e professionisti specializzati in tema di privacy e protezione dei dati personali, è in grado di condurre le imprese e i professionisti verso la conformità di legge, implementando le misure previste dal regolamento europeo. L'adeguamento normativo prevede una fase di set up iniziale (analisi; produzione documentale; prescrizione di misure e formazione obbligatoria) e una di mantenimento della conformità nel tempo, generalmente, annuale.

Il nostro team