PRIVACY FACILE: COME ADEGUARE LA PROPRIA IMPRESA ALLA NORMATIVA VIGENTE

Di Daniele Umberto Spano

Manuale pratico per l'applicazione della normativa vigente in tema di privacy alle piccole e medie imprese, ai professionisti e alle ditte individuali.

Dedica

Questo testo è dedicato a Fulvio Guatta, un caro amico venuto a mancare nel 2020. Fulvio ha ispirato il sottoscritto ed il mio socio, l'avv. Francesco Consoli, ad intraprendere questo complesso e intrigante tema della privacy. Lui era un grande esperto della materia ed è stato un consulente nella stesura, al tempo di Stefano Rodotà, primo garante della privacy dal 1997, dell'Allegato B, il documento, parte integrante della precedente normativa privacy, che definiva le misure idonee di sicurezza da applicare nella gestione dei dispositivi informatici utilizzati per il trattamento dei dati personali.
E' grazie anche a lui che oggi esiste Kruzer Srl, la società alla quale appartengo orgogliosamente.

Grazie Fulvio.

PRIVACY FACILE: COME ADEGUARE LA PROPRIA IMPRESA ALLA NORMATIVA VIGENTE di Daniele Umberto Spano© 2020

INDICE

Introduzione

GDPR: General Data Protection Regulation, ovvero Regolamento Generale per la Protezione dei Dati.
Questo acronimo, fino qualche tempo fa, patrimonio di pochi "esoterici" consulenti, è diventato estremamente diffuso e familiare a seguito della sua applicazione dopo il 24 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.
A sollevare ultimamente la questione privacy dei "dati sanitari" e "tracciamento", nell'era del Covid-19, disastrosa pandemia virale di quest'anno, il diffondersi delle applicazioni di tracciamento dei contatti, finalizzati alla prevenzione delle infezioni.
Il tema della privacy, spesso riferito ai clienti di un'organizzazione, 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.
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 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.
Il GDPR non si applica alle persone fisiche che trattano dati personali a scopo esclusivamente personale e alle forze dell'ordine, che rispondono ad altre normative specifiche.
Purtroppo, l'obbligatorietà dell'applicazione del Regolamento e le nuove disposizioni non sempre semplici da interpretare, hanno generato il fiorire di molti consulenti improvvisati, non sempre correttamente formati sulla materia.
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.

Perché un altro manuale?

Sul mercato esistono svariati testi sull'argomento, anche molto completi ed esaustivi, ma non sempre facilmente utilizzabili al fine di implementare, in modo pratico e sicuro nella propria azienda, tutti quei processi, documenti e policy richiesti dalla normativa.
Immaginiamo, per esempio, il titolare di un pubblico esercizio o di una piccola impresa, alle prese con un testo ricco di terminologia giuridica, teorie complesse e articoli di legge.
L'obiettivo di questo manuale è quello di fornire una visione chiara e semplificata delle più comuni problematiche affrontate nella fase dell'adeguamento dell'impresa, affrontando alcuni temi "erga omnes" e altri più specifici di alcune categorie merceologiche.
Questo manuale rappresenta un punto di riferimento per chi, pur avendo già effettuato l'adeguamento, intende verificare il lavoro svolto o approfondire alcuni temi specifici (ad es.: videosorveglianza, geo localizzazione, policy aziendali, etc.), e per chi affronta, per la prima volta, il tema della conformità al regolamento europeo nella propria organizzazione.
Il lettore può utilizzare il testo come un manuale operativo da consultare nel momento in cui ne ha bisogno.

L'autore del testo:

Daniele Umberto Spano
è nato a Milano, il 27 aprile 1966.
Negli anni ha rivestito il ruolo di imprenditore e, in passato, come consulente in diverse realtà, in particolare, nei settori della tutela del credito, del credito a consumo e della consulenza d'impresa e ha operato per imprese quali: Dun And Bradstreet Kosmos S.p.a.; Citifin S.p.a., gruppo Citibank; Findomestic S.p.a.
Dal 2015 si occupa specificamente di temi inerenti la cybersecurity ed il trattamento dei dati personali.
E', attualmente, amministratore, formatore e co-fondatore di Kruzer S.r.l., società di consulenza, specializzata in tema di privacy, costituita nel 2017. Effettua sessioni di formazione ai clienti e riveste il ruolo di DPO (Responsabile della Protezione dei Dati) per diverse realtà aziendali.

Kruzer Srl

Kruzer è una società frutto delle competenze tecnico legali di un team di avvocati specializzati in privacy e tecnici esperti di cybersecurity. Nasce nel 2017 con la mission di diventare una società leader nell'adeguamento al GDPR e nella consulenza in generale in tema di privacy.
La clientela è composta da aziende e professionisti nel nord Italia, operanti nei più svariati settori merceologici.

Maggiori informazioni nel sito: www.kruzer.it

Glossario

Di seguito, i principali termini appartenenti al vocabolario della privacy, utilizzati nel testo.

Accountability

Esprime il concetto di "responsabilizzazione" del *titolare dei trattamenti*, il quale è chiamato a rendere conto di tutto il processo di trattamento dei dati personali che tratta, per tutto il loro "percorso", dalla raccolta alla diffusione a terzi.

Amministratore di sistema

Persona interna o esterna all'azienda che si occupa dell'applicazione di tutte le buone pratiche relative alla gestione del sistema informatico dell'impresa, ivi compresa la sicurezza.

Audit

Analisi periodica dello stato di conformità dell'organizzazione rispetto alla normativa vigente.

Base giuridica

Elemento giuridico (art. 6 del GDPR) che rende lecito il trattamento di determinati dati personali. Esempi di *base giuridica:* consenso al trattamento dei dati; leggi nazionali; *legittimo interesse*; etc.

Big data

Dati disomogenei, provenienti da fonti diverse, generalmente in rete, che, una volta aggregati ed elaborati, consentono di creare dei profili personali.

Codice privacy italiano

Inizialmente definito dal D.lgs. 196/2003 come applicazione italiana della direttiva europea per la privacy, oggi novellato dal D.lgs. 101/2018 al fine di armonizzare il regolamento europeo (Gdpr) all'ordinamento italiano.

Consenso al trattamento

Definito come una *base giuridica* (art.6 del GDPR) per il trattamento di alcuni dati personali per determinate finalità. Deve essere esplicito; obbligatorio per alcune finalità (*profilazione*, marketing, utilizzo di dati non sempre fondamentali per l'esecuzione del contratto, etc.) e per il trattamento di *dati particolari* (sensibili).

Consulente privacy o privacy officer

Esperto di privacy, generalmente esterno all'impresa, che segue il cliente nella formazione, adeguamento e *audit* in tema di privacy.

Contitolare dei trattamenti

Entità e/o persona fisica che condivide, insieme al *titolare dei trattamenti*, il ruolo e la responsabilità di decidere quali dati personali trattare e per quali finalità. Generalmente, un contitolare è un fornitore di beni o servizi che condivide una fornitura complessa che richiede più attori. Per esempio: un portale di organizzazione di viaggi sarà contitolare dei dati dei clienti con hotel, compagnie aeree, società di autonoleggio, etc.

Cybersecurity

Sicurezza informatica. E' riferita ai dispositivi informatici di trasmissione/ricezione; conservazione ed elaborazione di dati (server; reti; pc; smartphone; etc.)

Data breach

Violazione di dati. Si riferisce ad eventi che possono inficiare le tre qualità indispensabili per il trattamento del dato: riservatezza; integrità e disponibilità. Può essere rappresentato da un furto, fisico o informatico, da malfunzionamenti di dispositivi, virus informatici, etc. Al suo verificarsi, il regolamento europeo prevede un iter di attività ben precise (artt. 33-34).

Dati biometrici

Dati personali riferibili a inequivocabili caratteristiche fisiche che rendono riconoscibile un individuo, come, ad esempio, l'immagine del volto, le impronte digitali, l'immagine della cornea, etc.

Dati comuni

Dati non relativi a persone fisiche.

Dati particolari

Dati personali relativi alla sua sfera privata e intima, come ad esempio: il credo religioso, lo stato di salute, lo stato finanziario, le preferenze sessuali, etc.

Dati personali

Dati che in forma singola o aggregata consentono, in modo univoco, l'identificazione di una persona fisica e alcune sue caratteristiche.

Defacement

Attività illecita, effettuata nel web da malintenzionati, che consiste nel ricreare un sito web identico a quello originale, per carpire dati e credenziali personali.

Designato, autorizzato o incaricato al trattamento dei dati

Persona fisica, generalmente collaboratore di un'impresa, incaricato da quest'ultima a trattare dati di terzi per suo conto.

Dpia o valutazione di impatto privacy

Documento imposto dal regolamento europeo sulla privacy (art. 35) per alcune tipologie di trattamento massivo dei dati, effettuate attraverso processi automatizzati o particolarmente rischiosi per le libertà e i diritti fondamentali dei soggetti interessati, in particolare se questi ultimi appartengono a categorie vulnerabili.

Dpo o Rpd (Responsabile Protezione Dati)

Persona incaricata di supervisionare tutti i processi di conformità delle imprese alla normativa sulla privacy. Il Dpo riveste il ruolo di intermediario tra l'impresa, il Garante privacy e i soggetti interessati. Deve essere esperto di privacy e non avere ruoli di conflitto d'interesse nel trattamento dei dati, quindi non può essere *l'amministratore di sistema* o un manager dell'azienda. La figura è prevista, in casi specifici, dal GDPR (art. 37).

Firewall

Dispositivo hardware o software di difesa perimetrale di una rete informatica. Si comporta da "filtro" per evitare intrusioni non autorizzate ai dispositivi della rete aziendale.

Gdpr o Rgpd

Acronimo di: General Data Protection Regulation o Regolamento Generale per la Protezione dei Dati. Si riferisce al regolamento europeo sulla privacy, il Reg. EU 679/2016.

Geolocalizzazione

Sistema, formato da dispositivi collegati ad una rete, che consente di localizzare una persona, un veicolo, un telefono o un pc, individuando in modo preciso la località geografica. Molto spesso viene utilizzato su veicoli aziendali.

Hacker

Definisce una persona in grado di ottenere informazioni riservate, accedendo, in modo non autorizzato, a sistemi informatici protetti. Spesso, il termine viene utilizzato impropriamente per definire chi danneggia files e sistemi. Questi ultimi, sono invece chiamati *cracker.*

Informativa

Documento reso pubblico dai *titolari e dai responsabili dei trattamenti* (artt. 13-14 del GDPR) per ottemperare al principio della trasparenza. Il documento riporta che dati vengono trattati, per quanto tempo, con quali *basi giuridiche,* con quali finalità, etc. Riporta anche tutti i diritti dei soggetti interessati.

Legittimo interesse

E' una delle *basi giuridiche* (art.6 del GDPR) di riferimento per il trattamento di alcuni dati. Implica un bilanciamento di interessi tra il *titolare dei trattamenti* ed il *soggetto interessato.* E' la *base giuridica* utilizzata, per esempio, per la ripresa video delle telecamere di sicurezza a scopo di tutela del patrimonio o dei trattamenti dei dati da parte di chi recupera i crediti.

Log management

Sistema di tracciamento di tutte le attività all'interno di dispositivi informatici. Il sistema di Log Management consente di supervisionare accessi, modifiche, cancellazioni e trasferimenti di dati all'interno di server, pc, etc., indicando chi e quando ha effettuato tali attività.

Misure adeguate – tecniche ed organizzative

Insieme di tutti gli interventi riguardanti l'organizzazione, la formazione, la documentazione e l'implementazione di sistemi informatici e fisici, atti a garantire la massima tutela e protezione dei dati.

Phishing

Pratica malevola, attuata da criminali informatici, allo scopo di ottenere dati e informazioni dagli utenti con l'inganno, per utilizzarli a loro profitto. Generalmente, si tratta di user ID e password, ma la tecnica può essere utilizzata per ottenere anche altre informazioni utili a realizzare truffe.

Policy

Regolamento aziendale condiviso che definisce comportamenti, procedure e regole per l'utilizzo di mezzi e servizi dell'azienda da parte del personale incaricato.

Privacy by default

Uno dei principi su cui si deve basare l'organizzazione della privacy dei dati personali in azienda: "su regole di sicurezza e tutela di base definite".

Privacy by design

Uno dei principi su cui si deve basare l'organizzazione della privacy dei dati personali in azienda: progettare qualsiasi nuovo trattamento tenendo conto, fin dalla fase di progettazione, delle regole e dei principi di tutela dei dati.

Profilazione

Processo che prevede la raccolta e l'elaborazione di una serie di dati personali, allo scopo di ottenere una "mappatura" della persona, in grado di definirne gusti, comportamenti, orientamenti, situazione economica, età, stato civile, etc. La profilazione può essere effettuata a scopo commerciale e di marketing; per determinare la finanziabilità e l'affidabilità finanziaria di un soggetto; per determinare un quadro clinico; etc. Tranne che in alcuni casi particolari, la profilazione è possibile solo attraverso l'espressione di un consenso specifico del soggetto interessato.

Registro dei trattamenti

Adempimento previsto dal GDPR (art.30). E' la mappatura con tutte le caratteristiche specifiche, di tutti i trattamenti di dati personali effettuati nella propria organizzazione.

Responsabile esterno del trattamento

Ruolo previsto dal GDPR (art. 28). Si tratta di persona o entità giuridica, economica o pubblica che tratta i dati di soggetti per conto del titolare dei trattamenti. Per esempio, il consulente del lavoro, tratta i dati dei dipendenti di una società, per conto del suo titolare.

Soggetto interessato

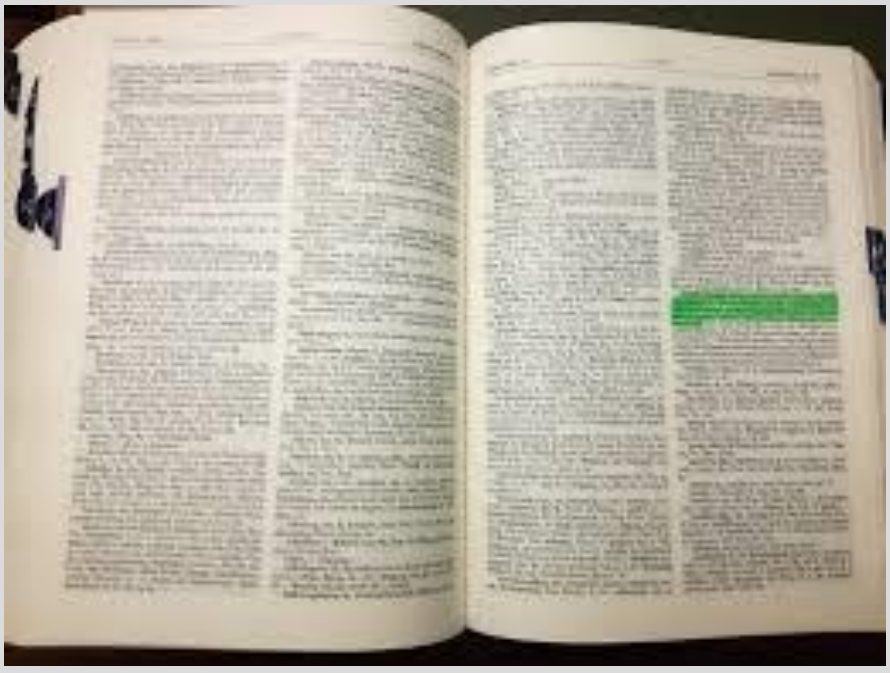
Persona fisica al quale i dati trattati appartengono.

Titolare dei trattamenti

Persona fisica o entità giuridica, economica o pubblica che determina quali sono i dati da trattare e le loro finalità.

Trattamento dei dati

Qualsiasi processo di intervento sui dati: raccolta, accesso, conservazione, cancellazione, modifica, diffusione, confronto, elaborazione, condivisione, etc.



Il Gdpr in una pagina: panoramica sintetica dei punti principali del regolamento europeo (Reg. Eu 679/2016)

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) 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.

I dati personali e i dati particolari

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, ecc..

Particolarmente importanti sono:

• i **dati che permettono l'identificazione diretta** - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i **dati che permettono l'identificazione indiretta**, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);

• i **dati rientranti in particolari categorie**: si tratta dei dati c.d. *"sensibili"*, cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il **Regolamento (UE) 2016/679** (articolo 9) ha incluso nella nozione anche i **dati genetici,** i **dati biometrici** e quelli relativi all'**orientamento sessuale**;

• i **dati relativi a condanne penali e reati**: si tratta dei dati c.d. *"giudiziari"*, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il **Regolamento (UE) 2016/679** (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Con l'evoluzione delle nuove tecnologie, **altri dati personali** hanno assunto un ruolo significativo, come **quelli relativi alle comunicazioni elettroniche** (via Internet o telefono) e **quelli che consentono la geolocalizzazione**, fornendo informazioni sui luoghi frequentati e sugli spostamenti."

Importanza dell'adeguamento

Il tema del trattamento dei dati personali, negli anni dei social, del marketing aggressivo e delle problematiche legate alla sicurezza informatica, assume un ruolo di primo piano, sia per i soggetti interessati, cioè le persone oggetto dei trattamenti, sia per chi i dati li deve trattare, quindi le aziende, gli enti pubblici, le associazioni e tutte le entità presenti nel panorama economico e amministrativo delle nazioni che trattano i dati dei cittadini europei.

In Italia, purtroppo, al contrario che in altri paesi, si è spesso sottovalutata la questione privacy, derubricandola ad un mero esercizio burocratico.

In realtà, la definizione "regolamento sulla privacy" è la semplificazione di un concetto più ampio, già esplicitato dal significato dell'acronimo "Gdpr": General Data Protection Regulation, cioè Regolamento Generale per la Protezione dei Dati. La "protezione" del dato riguarda la sua raccolta, la sua conservazione, la sua diffusione, il suo utilizzo e, in generale, qualsiasi tipo di trattamento che lo riguarda.

Diventa, quindi fondamentale, porre l'accento su quali vengono trattati, con quali finalità e in che modo.

Adeguare la propria organizzazione alle normative vigenti consente, oltre che evitare eventuali sanzioni, di ottenere una serie di vantaggi, come ad esempio:

- Aumentare la produttività, grazie ad una corretta riorganizzazione dei flussi informativi e del sistema informatico;
- Tutelarsi da eventuali controversie da parte di clienti, di collaboratori o di altri soggetti, grazie all' implementazione di misure preventive, come le policy aziendali, gli accordi di riservatezza e la corretta contrattualistica;
- Ottenere la possibilità di partecipare a gare d'appalto indette da soggetti pubblici o privati che richiedono la prova della conformità rispetto al regolamento in vigore;
- Guadagnare una buona reputazione, dimostrando di avere cura dei dati personali di clienti e collaboratori;
- Evitare il più possibile accessi indesiderati ai dati, il loro utilizzo illecito o il loro danneggiamento, come conseguenza di azioni di violazione di sistemi informatici o furti di pc, server e hard disc;
- Aumentare la consapevolezza dei propri collaboratori rispetto ai rischi informatici e quindi all'utilizzo più attento delle strumentazioni informatiche aziendali.

Le ispezioni effettuate in Italia e in altri paesi UE e le relative sanzioni comminate hanno dimostrato una grande attenzione nei confronti dei processi aziendali e della protezione dei sistemi informatici. Ciò non significa che le nomine di responsabilità, le informative corrette e tutto il resto della documentazione prodotta non siano elementi importanti, al contrario, ma, certamente, non possono che rappresentare solo una parte del processo di adeguamento alla normativa.

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.

Valutare lo stato dell'arte della propria impresa rispetto al regolamento europeo

Proponiamo, qui sotto, una check list finalizzata a verificare l'adeguatezza alle nuove normative sulla privacy, della propria organizzazione. Si tratta, naturalmente, di un iter semplificato adatto a organizzazioni non troppo complesse. Realtà più complesse e strutturate necessitano certamente di interventi più specifici, anche in loco, a cura di professionisti esperti.
Gli imprenditori o i loro designati possono, rispondendo alle domande sotto elencate, capire se hanno già, almeno in parte affrontato il percorso dell'adeguamento. I temi, qui solo accennati, saranno ripresi e sviluppati nel capitolo "Adeguamento della propria impresa al GDPR (per tutte le imprese)" e nei capitoli specifici dedicati alle specifiche categorie merceologiche.

DOMANDE	RISPOSTE
1) E' stata prodotta la documentazione necessaria? I documenti che devono essere prodotti sono i seguenti: - elenco di tutti i dispositivi che trattano dati personali (pc, server, telecamere, armadi, schedari, etc.); - analisi dei rischi privacy con descrizione delle misure tecniche e organizzative da implementare; - valutazione di impatto privacy sui diritti e le libertà dei soggetti interessati; - registro dei trattamenti; - nomine di autorizzazione e di responsabilità esterna dei trattamenti; - informative specifiche (clienti, dipendenti, fornitori, visitatori, videosorveglianza, candidati, sito web, etc.) e relativi moduli di consenso; - documentazione integrativa: policy aziendali; integrazioni contrattuali; impegni alla riservatezza; moduli di comodato di smartphone e tablet; etc. analisi documentazione e autorizzazioni privacy; documenti inerenti il diritto del lavoro; altro) se in presenza di particolari trattamenti di dati (esempio: videosorveglianza; geolocalizzatori; controllo accessi con dati biometrici; trattamento di dati personali di persone vulnerabili, come minori, malati, etc.)	o Si' o No o In corso di implementazione
2) E' stata effettuata un'accurata analisi dello stato di sicurezza delle infrastrutture informatiche e fisiche e l'implementazione di procedure e/o tecnologie adeguate, anche per la continuità dell'attività aziendale? Le recenti ispezioni e le linee guida, dimostrano che la conformità documentale non è l'unico elemento da considerare, dato che, come specificato nel regolamento europeo, la principale responsabilità del titolare dei trattamenti è quella di implementare tutte le misure tecniche e organizzative idonee alla tutela e alla protezione dei dati personali dei soggetti interessati. Password adeguate, antivirus, firewall e tutti i dispositivi hardware e software rappresentano solo una parte di misure tecniche da implementare. Per gli archivi "fisici", come gli armadi e gli archivi, si dovranno prevedere altre misure atte a limitarne l'accesso alle persone non autorizzate.	o Si' o No o In corso di implementazione
3) E' stata effettuata la formazione obbligatoria di tutti i soggetti che nella propria organizzazione trattano dati personali? Nel GDPR, l'art. 29, impone che tutti i soggetti, che all'interno della organizzazione trattano dati personali, vengano formati sui principi generali del regolamento e su tutte le buone pratiche che consentano l'applicazione degli stessi nella quotidianità dell'attività aziendale. Al momento non esiste un protocollo preciso da seguire, né attestati o certificazioni, in quanto, in caso di ispezione, è necessario dimostrare che le persone incaricate ai trattamenti di dati siano, di fatto, preparate e applichino pedissequamente il regolamento. In ogni caso, produrre attestati di frequenza a specifici corsi o qualsiasi elemento che provi la formazione effettuata può agevolare la dimostrazione dello stato di conformità formativa.	o Si' o No o In corso di implementazione
4) L'organizzazione aziendale è strutturata per consentire ai soggetti interessati di esercitare i propri diritti? Il GDPR, oltre a riproporre i diritti dei soggetti interessati già previsti dalla normativa precedente, ne prevede di nuovi. E' fondamentale che, all'occorrenza, sia possibile, in tempi ragionevoli e comunque non superiori ai 30 giorni, soddisfare la richiesta dei soggetti interessati rispetto alla modifica, la cancellazione, l'opposizione al trattamento e, in generale, qualsiasi azione inerente la gestione dei dati personali.	o Si' o No o In corso di implementazione
5) Per il trattamento dei dati personali, sono state definite le corrette "basi giuridiche"? La base giuridica stabilisce la condizione che rende lecito un trattamento di dati. Alcuni esempi di basi giuridiche sono: il consenso; una legge nazionale; il legittimo interesse.	o Si' o No o In corso di implementazione

Le basi giuridiche vanno indicate all'interno dell'informativa, in relazione alle tipologie di dati trattati e, in alcuni casi, incidono sull'organizzazione aziendale. Per esempio, se la base giuridica, per un determinato trattamento (ad esempio, l'invio di mail promozionali) fosse il consenso dei soggetti interessati, sarebbe opportuno porre in essere un sistema di raccolta, conservazione e aggiornamento dei consensi efficiente e funzionale all'attività da svolgere.	o Si' o No o In corso di implementazione o Non applicabile
6) Si gestisce utilizzando le corrette basi giuridiche e i principi di sicurezza la diffusione di dati personali verso paesi extra UE? Dopo un'analisi delle finalità, del paese in questione e del processo utilizzato, si definirà se è necessario o meno il consenso esplicito del soggetto interessato. Inoltre, bisognerà, nei limiti del possibile, garantire una gestione sicura dei dati verso tali paesi.	o Si' o No o In corso di implementazione o Non applicabile
7) Sono stati definiti i ruoli di incarico e responsabilità all'interno e all'esterno della propria organizzazione? Il titolare dei trattamenti, cioè l'azienda o il professionista, nella maggior parte dei casi, si avvale di figure interne (collaboratori; dipendenti) che devono essere nominati "autorizzati al trattamento", previo adeguato percorso formativo specifico, e di figure esterne, come consulenti o aziende (commercialista; consulente del lavoro; etc.) che vanno nominati "responsabili esterni dei trattamenti". Questo è indispensabile, in quanto, a tali soggetti, vengono trasmessi dati personali di soggetti terzi (dati dei propri clienti, fornitori e dipendenti). Nel caso in cui i dati fossero trattati da più soggetti giuridici, può delinearsi il concetto di "contitolarità" dei trattamenti. Altri incarichi formali possono riguardare la nomina di "designati", per alcuni specifici trattamenti (ad esempio, il designato della videosorveglianza, il designato alla privacy, etc.) e l'amministratore di sistema, per quanto concerne la gestione delle infrastrutture informatiche.	o Si' o No o In corso di implementazione o Non applicabile
8) Sulla base dei ruoli aziendali, è stata definita la modalità di accesso ai dati di specifica competenza e un sistema di "log management"? In molte organizzazioni, una parte ampia del personale è in grado di trattare dati inutili per la propria mansione, spesso, perché esiste un accesso diffuso a software gestionali o a server condivisi. Un sistema di "log management" consente di "tracciare" il soggetto che ha avuto accesso a determinati database.	o Si' o No o In corso di implementazione o Non applicabile
9) Vengono effettuati trattamenti che prevedono decisioni automatizzate che possono determinare la fruibilità di un servizio, come ad esempio, l'accesso al credito? Vengono effettuate profilazioni (insieme di caratteristiche, abitudini, gusti, etc. che definiscono una tipologia di cliente/utente)? Vengono gestiti grandi quantità di dati: di categorie vulnerabili (minori, malati, etc.); attraverso tecnologie innovative? Nel caso in cui fosse vera una di queste condizioni, è stata effettuata una valutazione d'impatto privacy (DPIA)? La valutazione d'impatto sostituisce, per alcuni particolari trattamenti di dati, la richiesta da effettuare all'ufficio del Garante della privacy.	o Si' o No o In corso di implementazione
10) E' stata definita la necessità o meno di nominare un Responsabile della Protezione Dati (DPO)? Nei casi di trattamenti massivi di dati personali o di trattamenti di dati particolarmente sensibili, in via continuativa, la normativa prevede che venga istituita la figura del DPO (Data Protection Officer) (Artt. 37-39).. Il DPO è una sorta di supervisore della privacy aziendale ed è colui che, fungendo da trade union tra l'ufficio dell'Autorità Garante e l'azienda, da una posizione di neutralità, svolge azioni di auditing, formazione, verifica, consulenza e di contatto con i soggetti interessati di cui il Cliente è titolare dei trattamenti.	o Si' o No o In corso di implementazione
10) E' stata definita la procedura della gestione di eventuali violazioni, incidenti e anomalie, riferite ai dati personali, come previsto dal regolamento? Due articoli del GDPR, il 33 il 34, definiscono chiaramente come devono essere gestite le situazioni, come un episodio di violazione informatica, di un furto di dati o, in generale, di un incidente che inficia la riservatezza, l'integrità o la disponibilità dei dati personali.	

Adeguamento della propria impresa al GDPR (per tutte le imprese)

In questa sezione del manuale, iniziamo ad affrontare tutti gli steps indispensabili per iniziare il percorso verso l'adeguamento della propria struttura alla nuova normativa vigente sulla privacy.
Le istruzioni riportate valgono per la maggior parte delle organizzazioni. Ulteriori temi di approfondimento sono presenti nelle sezioni specifiche dedicate alle singole categorie merceologiche.
Consigliamo di seguire il processo punto per punto, nell'ordine proposto e, una volta effettuato l'adeguamento, ripercorrere tutti gli steps per verificare se tutte le sezioni sono state completate, in particolare, dopo aver consultato i capitoli del manuale riportanti le istruzioni per la specifica categoria merceologica di appartenenza. Infatti, si potrebbero trovare spunti ed elementi da approfondire a completamento del lavoro di base.

Inizio del percorso di adeguamento

Step 1. Redigere un elenco di tutti i dispositivi fisici e informatici che trattano dati personali.

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
……	…..	……	……	……

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
……	…..	……	……	……

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

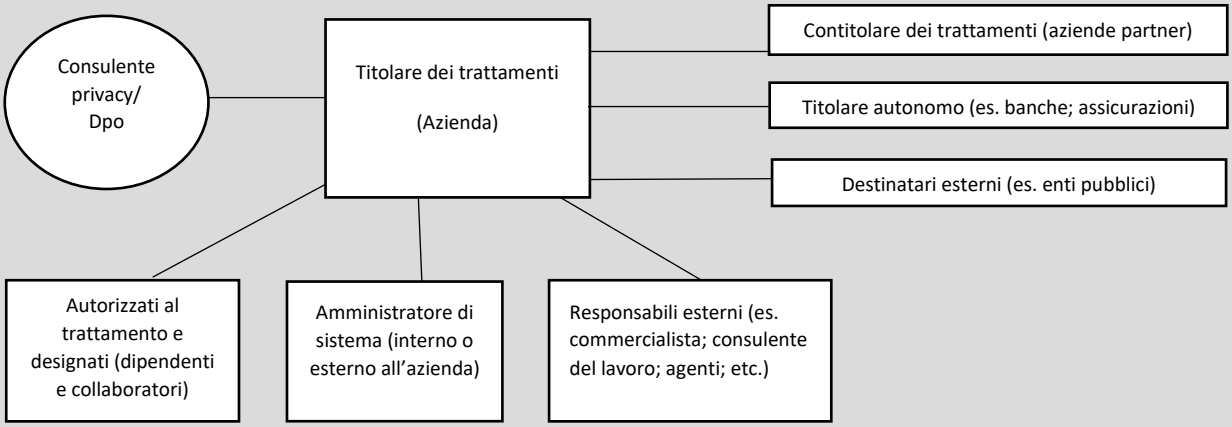
Tab 4

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, contributi, timbrature, ferie, etc.;	Responsabile esterno
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)

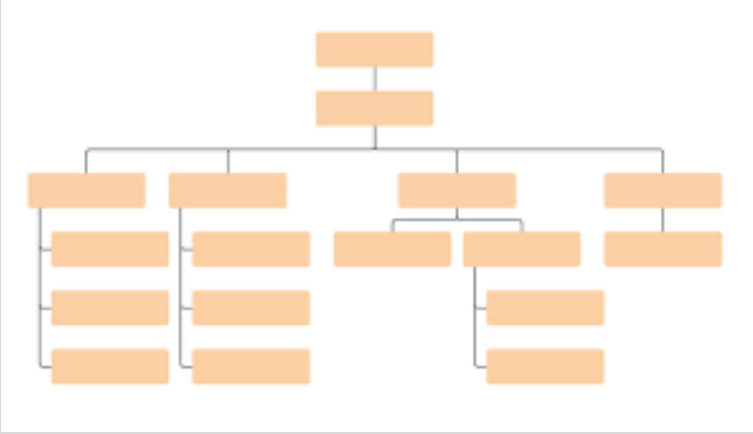


I ruoli dei vari soggetti, all'interno dell'*organigramma privacy,* possono essere regolamentati da semplici autorizzazioni, come nel caso degli autorizzati al trattamento (tipicamente, dipendenti e collaboratori), o da atti giuridici, come nel caso di responsabili esterni e di contitolari dei trattamenti. 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, riportate nelle tabelle 3 e 4, nel precedente paragrafo.

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 Pagina 3 di 4

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 Pagina 4 di 4

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: dati biometrici) 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)

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 più di 250 dipendenti, secondo il regolamento europeo, ma anche da chi ha anche solo un dipendente, secondo le linee guida emesse dal Garante italiano della privacy (anche se in forma molto ridotta), da chi tratta dati particolari (sanitari, giudiziari, etc.) e da chi, col trattamento di dati personali, potrebbe mettere a rischio le libertà e i diritti individuali.
Alcuni esempi pratici:
un'officina che ha un dipendente, deve redigere il registro; un negoziante senza dipendenti può non redigerlo; un parrucchiere, un tatuatore, un massaggiatore, anche senza dipendenti, trattando potenzialmente dati sulla salute (allergie, riscontro di patologie) devono redigerlo.
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 sottoriportate:

- 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 marketing); consenso per l'utilizzo del numero di cellulare come contatto.	Legittimo interesse del titolare
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.

Alcune attività, quelle che prevedono la nomina di responsabile esterno, dovranno redigere, oltre al registro "titolare", il registro "responsabile". La redazione sarà simile a quella dell'esempio illustrato ma il titolare indicato per il trattamento corrisponderà al nome delle aziende clienti e il responsabile esterno sarà l'azienda che redige il registro. I gruppi di trattamenti dipenderanno dall'attività svolta.

Le attività più comuni che prevedono la compilazione del registro e la nomina di responsabile esterno sono le seguenti:

commercialisti; consulenti del lavoro; amministratori di condominio; società di assistenza informatica/gestionali; società di medicina del lavoro; società di recupero del credito; società di cloud computing; società di elaborazione dati; gestori di app e portali web.

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.
Al momento della stesura del presente manuale, non esistono certificazioni specifiche che determinano la professionalità di un esperto di privacy, se non le classiche certificazioni di qualità ISO.

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.

Le basi della sicurezza fisica e 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. È bene 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.

La procedura in caso di *data breach.*

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.

La privacy dei dipendenti e i dispositivi aziendali

I primi soggetti con i quali un imprenditore si relaziona, trattandone i dati personali più delicati sono proprio i suoi dipendenti. L'affermazione non è così banale come sembra, dato che una delle prime domande che spesso gli imprenditori mi rivolgono è: "ma io cosa devo fare per la privacy, visto che vendo macchinari a grandi aziende? Io non tratto dati".
Un'altra precisazione doverosa riguarda un altro concetto, già ben compreso da chi ha letto i capitoli precedenti del manuale: gli adempimenti relativi alle normative sulla privacy prescindono dalla necessità di dover far firmare un consenso.

Quando abbiamo a che fare con il personale dipendente o che, anche in altre forme, collabora con noi, generalmente non ci sono consensi da far sottoscrivere per i seguenti motivi:
1) la maggior parte dei trattamenti di dati effettuati dal datore di lavoro nei confronti dei dipendenti hanno come base giuridica, non il consenso, ma l'esecuzione del contratto (nel caso specifico, il contratto di lavoro) e le leggi nazionali (previdenza; fisco; etc.);
2) qualsiasi giudice non darebbe valore alla firma di un dipendente in quanto il suo ruolo è considerato in condizione di soggezione rispetto al datore che potrebbe esercitare una qualche forma di coercizione nei suoi confronti;
3) nessuna firma o manifestazione di consenso può inoltre giustificare un utilizzo illecito o non giustificabile dei dati personali.

Ricorderemo più volte, all'interno dei singoli punti trattati, che è vietato il controllo a distanza del lavoratore. E' necessario fare molta attenzione anche all'applicazione di procedure di controllo atte a verificare come il collaboratore utilizzi i dispositivi aziendali. I controlli devono essere sempre:
- programmati;
- mai eccessivi nei tempi, nei modi e nelle finalità (le uniche finalità sono quelle della sicurezza dei dati);
- giustificati da finalità di sicurezza e protezione;
- riportati nelle policy aziendali;
- effettuati da personale designato e formato;
- non devono rappresentare una forma di controllo della persona;

Una recente sentenza ha scagionato un datore di lavoro che, giustificato da un fondato sospetto di furti in azienda, ha utilizzato delle telecamere nascoste. Tuttavia, la sentenza non rappresenta un "via libera" a trattamenti così invasivi svolti in piena libertà. Ricordiamo poi che le sentenze vengono emesse, oltre che secondo una sensibile discrezionalità interpretativa dei fatti e delle leggi, secondo l'analisi di moltissimi fattori che, spesso, gli organi di stampa omettono per sintesi.
.
I principi che regolano il rispetto della privacy dei dipendenti trovano forma giuridica sia nelle leggi che regolano il diritto del lavoro (legge 300 del 1970 aggiornata 2019), sia nelle leggi specifiche (Reg. Eu 679 del 2016; d.lgs. 101 del 2018).

I controlli e le verifiche effettuate dal datore sugli strumenti aziendali, in generale, sono vietati a meno che non esistano sospetti concreti di truffa, lesa immagine, concorrenza sleale e reati in genere o l'esigenza di difendersi in giudizio. La stesura di una policy condivisa e, in alcuni casi, di accordi sindacali con le RSA e le RSU delle aziende, può regolamentare verifiche finalizzate alla sicurezza e all'organizzazione aziendale, ma mai alla valutazione del lavoro del dipendente.

Le 10 questioni inerenti la privacy dei collaboratori più dibattute nelle aziende, generalmente sono le seguenti:

1) videosorveglianza;
2) localizzatori gps;
3) utilizzo dei dispositivi informatici aziendali;
4) utilizzo dei dispositivi propri in ambito aziendale/lavorativo;
5) sistemi di timbratura/controllo degli accessi;
6) trattamento di dati particolari (dati: sulla salute; sulla situazione familiare; sui gusti sessuali; sulle opinioni politiche; etc.);
7) trattamento di dati giudiziari;
8) controllo dei dati di navigazione in rete;
9) trattamento e diffusione/utilizzo illecito di dati aziendali riservati da parte dei collaboratori.

Analizziamole punto per punto:

1) Videosorveglianza.

Come già riportato nel capitolo dedicato alla videosorveglianza, il trattamento, prima di essere effettuato (meglio se prima dell'installazione delle telecamere) necessita dell'autorizzazione della rappresentanza sindacale o dell'Ispettorato del lavoro. Non è necessario richiedere il consenso ai singoli collaboratori, ma è importante informarli della presenza delle telecamere e della possibilità di prendere visione dell'informativa specifica.
Evitare di "puntare" le telecamere sulle postazioni di lavoro a meno che non ci siano esigenze specifiche rispetto alla sicurezza sul lavoro (macchinari e postazioni in ambienti ad alto rischio) o di particolare tutela del patrimonio (ad es. la cassa di un pubblico esercizio).
E' vietato utilizzare la videosorveglianza per il controllo a distanza dell'attività dei collaboratori.

2) Localizzatori gps.

Il tema è stato trattato in modo approfondito nel capitolo specifico. In generale, si applicano gli stessi principi della videosorveglianza: autorizzazione sindacale o dell'Ispettorato del lavoro; utilizzo dei dati minimale e solo per il tempo e le finalità definite (organizzazione del lavoro; sicurezza; clausole assicurative; etc.); informativa specifica. E' fondamentale che il collaboratore possa disinserire il localizzatore nei momenti di pausa dal lavoro.

3) Utilizzo dei dispositivi informatici aziendali.

L'utilizzo dei pc, degli smartphone, dei laptop, della posta elettronica, della navigazione web e di tutti quei dispositivi e servizi che l'azienda mette a disposizione dei collaboratori per lo svolgimento dell'attività, dovrebbe essere regolato e definito tramite specifiche *policy* e

regolamenti condivisi. Lo scopo delle *policy* è quello di chiarire quali siano i limiti e le modalità dell'utilizzo possibile dei dispositivi per garantire la massima sicurezza del patrimonio aziendale e dei dati trattati, tutelando l'impresa e i diritti del datore di lavoro. E' fondamentale che nelle *policy* siano indicate tutte le buone pratiche da mettere in atto durante l'uso degli strumenti e le possibilità di controllo da parte del datore di lavoro o di un responsabile che, in ogni caso, deve fare attenzione a rispettare la privacy del collaboratore.

Di seguito alcuni punti da riportare nelle policy:
- è possibile definire un limite rispetto all'utilizzo della navigazione web e della posta elettronica che deve essere utilizzata solo allo scopo di svolgere l'attività aziendale;
- vietare l'installazione di software, applicazioni e file, nonché l'utilizzo di porte usb o il collegamento di dispositivi personali ai dispositivi aziendali senza l'autorizzazione dell'azienda;
- regolamentare l'utilizzo dei telefoni aziendali. L'utilizzo a scopo personale deve essere autorizzato dal datore di lavoro;
- avvisare il collaboratore rispetto alla possibile verifica dell'utilizzo dei dispositivi da parte del datore di lavoro.

Un'attenzione particolare deve essere posta rispetto a quest'ultimo punto. I controlli periodici di routine possono essere effettuati sui dispositivi aziendali ma facendo attenzione a non violare la privacy del collaboratore e a non trasformare la "verifica" di sicurezza in un controllo serrato dell'attività della persona. Questo tipo di comportamento potrebbe essere causa di ricorsi sindacali.
Il traffico telefonico può essere verificato, richiedendo i tabulati alla società telefonica, al fine di ottimizzare i costi scegliendo gli operatori più convenienti o per effettuare controlli in caso di fondati sospetti. In ogni caso, sono da evitare controlli continui e regolari e l'utilizzo dei dati deve essere minimo e limitato nel tempo.
Se il pc del dipendente, per motivi di sicurezza e di verifica generale, può essere visionato dal datore di lavoro, la mail aziendale del dipendente, come pure qualsiasi altra applicazione di messaggistica, non può essere consultata da nessun'altra persona, se non dal suo intestatario. Su questo si è espresso anche il Garante della privacy. Inoltre, in caso di licenziamento, l'account deve essere immediatamente chiuso. Al fine di tutelare la ricezione della posta diretta all'azienda, il datore di lavoro può attivare una sorta di "risponditore" automatico che informa i mittenti del cambio dell'indirizzo di riferimento.
E' consigliabile utilizzare, quando possibile, account aziendali "generici", tipo assistenza@azienda.it, specificando sempre, all'interno di una policy, che la casella, deve essere utilizzata solamente per alcune finalità specifiche e che può essere consultata, in caso di assenza per malattia o ferie da alcune persone dell'azienda designate allo scopo.
E' comunque fondamentale informare preventivamente l'utilizzatore della casella su chi, come e quando può utilizzarla.

4) Utilizzo dei dispositivi propri in ambito aziendale/lavorativo

Non rappresenta la situazione ottimale (sarebbe bene che l'azienda mettesse a disposizione tutto l'occorrente), tuttavia può capitare, in via emergenziale (un esempio è stato il ricorso allo *smart working* durante il lockdown imposto durante la pandemia del Covid 19) che il collaboratore si trovi ad utilizzare dispositivi proprietari.
Ovviamente, il datore di lavoro, in questo caso, non può imporre particolari restrizioni ma può imporre che i dati, il cui trattamento è titolarità dell'azienda, siano trattati secondo regole ben definite, in modo da garantirne la riservatezza, l'integrità e la disponibilità.
Un caso tipico è l'utilizzo dello smartphone e del laptop.
Ricordiamo che un dispositivo connesso alla rete intranet aziendale potrebbe essere una potenziale fonte di rischio di infezione informatica, se non sono state prese tutte le dovute precauzioni.
La *policy* finalizzata alla regolamentazione dell'utilizzo dei dispositivi, dovrebbe comprendere l'eventualità dell'utilizzo di strumenti propri, ma anche, in alcuni casi, il divieto di utilizzo di strumenti propri connessi alla rete aziendale o per il trattamento di dati aziendali.
Un approfondimento relativo a questi temi, ma legati al telelavoro, è disponibile nel capitolo "Il telelavoro".

5) sistemi di timbratura/controllo degli accessi

Il controllo degli accessi e delle presenze sono regolamentate secondo la base giuridica del "legittimo interesse" del titolare del trattamento. I dati devono essere, come sempre, trattati seguendo le corrette modalità per la loro protezione ed utilizzo, limitati nella diffusione, accessibili ed eliminati quando ne viene meno il loro utilizzo.
Nel caso di installazione di sistemi di verifica tramite: riconoscimento facciale; impronte digitali; lettura della cornea o, in generale, utilizzando dati biometrici necessitano della *valutazione di impatto privacy* e dell'implementazione di tutte le modalità e le soluzioni tecnologiche atte a mitigarne i potenziali rischi riscontrati.

6) trattamento di dati particolari (dati: sulla salute; sulla situazione familiare; sui gusti sessuali; sulle opinioni politiche; etc.)

I dati particolari, generalmente, non si possono trattare a meno che non ci sia un consenso esplicito o un motivo specifico. Alcuni esempi: l'informazione riguardo la religione di un dipendente, sarà trattata dal datore, non come elemento di discriminazione, ma per agevolare la persona nel praticare riti e nel rispettare festività particolari; la dichiarazione del dipendente rispetto all'assistenza dovuta ad un familiare bisognoso, sarà finalizzata all'attuazione delle agevolazioni della legge 104 e all'organizzazione aziendale durante l'assenza e così via. I dati sulla salute saranno trattati esclusivamente e in qualità di *titolare autonomo dei trattamenti* dal medico competente. Il datore di lavoro avrà il diritto e il dovere di conoscere solo l'idoneità del lavoratore all'attività svolta.

7) trattamento di dati giudiziari

Alcune professioni particolari, come lo svolgimento di servizi di vigilanza, di mediazione creditizia, etc., implicano l'obbligo di richiedere il casellario giudiziale e i carichi pendenti dei collaboratori. In questo caso, la base giuridica è una legge nazionale, quindi i dati non solo si possono, ma si devono trattare. Rimangono sempre validi i principi, già espressi, di tutela, sicurezza, garanzia di riservatezza, oblio, etc. Senza una motivazione legata ad una legge in vigore o all'esercizio di particolari diritti del soggetto interessato, questi dati non si possono trattare liberamente.

8) controllo dei dati di navigazione in rete

Anche in questo caso, come per il controllo sui pc e sulle mail, il controllo sistematico è vietato. I controlli devono essere motivati da concreti sospetti di reato, sicurezza aziendale e ottimizzazione delle procedure e dei sistemi. E' raccomandabile la redazione di una policy condivisa.

9) trattamento e diffusione/utilizzo illecito di dati aziendali riservati da parte dei collaboratori.

Come già accennato, un sospetto concreto di reato o di comportamento che genera danno legale, economico o di immagine all'azienda, giustifica controlli e verifiche. E' comunque consigliabile il ricorso ad un consulente legale così da svolgere le azioni di controllo nei tempi e nei modi corretti. E' anche ammesso l'incarico ad un investigatore privato per investigare e raccogliere prove sui comportamenti scorretti del collaboratore.
Ricordiamo che le prove estratte da dispositivi informatici devono essere raccolte e conservate seguendo la corretta catena di custodia prevista dalla legge. In caso contrario, le prove potrebbero essere nulle in tribunale.
Evitare, quindi, nel caso in cui si dovessero estrapolare dei dati da un dispositivo informatico, di avvalersi di comuni consulenti informatici, ma consultare degli esperti informatici forensi.

Controlli più approfonditi sul dipendente "infedele", se giustificati da un reale sospetto, è bene delegarli ad un investigatore privato che, godendo di speciali autorizzazioni da parte delle prefetture, è in grado di indagare sulle persone, utilizzando mezzi e tecniche particolari, non consentite al comune cittadino.

La gestione dei dati dei minori e di categorie vulnerabili

Alcune società potrebbero avere l'esigenza di trattare dati di soggetti minorenni, pensiamo ad asili pubblici e privati; tour operator che gestiscono viaggi per gite scolastiche; istituti scolastici; medici; palestre; cooperative di servizi sociali; etc.
Quali sono, in questo caso, le procedure da implementare?
Prima di tutto, è bene definire cosa si intende per minore età. Infatti, secondo il regolamento europeo, i soggetti interessati sono autonomi a livello decisionale sulla privacy, a partire dall'età di 14 anni. Ogni paese dell'Unione ha poi fatto la sua scelta. In Italia, l'età di 14 anni rappresenta la soglia per esercitare il proprio diritto di consenso al trattamento dei dati nella "società dell'informazione" (Internet e social media), mentre, nella società "reale" l'età di riferimento è quella dei 16 anni.
Al di sotto di questi limiti di età è necessaria la sottoscrizione di entrambi i genitori o i tutori legali.
E' concesso l'intervento di un solo genitore se devono essere esercitati i diritti alla privacy per le attività "ordinarie" e indispensabili, come il diritto alla scuola, alle cure mediche, etc. o se l'intervento del secondo genitore è oggettivamente impossibile per motivi di forza maggiore.

Alcune criticità, vista la delicatezza dei dati trattati, potrebbero emergere anche nei trattamenti da effettuare per soggetti considerati "vulnerabili". Pensiamo a soggetti diversamente abili, persone con particolari patologie o appartenenti ad alcune categorie sociali, ad esempio, ex carcerati o persone con situazioni familiari particolari. Infatti, una violazione di tali dati potrebbe generare episodi di discriminazione, di reputazione e, in generale, di impatto grave sui diritti e sulle libertà fondamentali.
Le regole da applicare al trattamento sui minori e sulle categorie vulnerabili sono, in generale, le stesse degli altri trattamenti (minimizzazione; finalità lecite; conservazione limitata nel tempo; misure di sicurezza; etc.), ovviamente con una maggiore attenzione.

Se il trattamento dei dati di minori e di altre categorie vulnerabili è continuativo e su larga scala è indispensabile redigere una *valutazione di impatto privacy (dpia)* (vedi capitolo "Adeguare la propria impresa in dieci mosse") e inserire nel *registro dei trattamenti* le tipologie di trattamento effettuate su questi soggetti.
E' probabile che molte attività di trattamento rivolte a queste persone, quando vengono effettuate per finalità conseguenti al loro specifico status, richiedano la base giuridica del *consenso esplicito* in quanto è implicito che siano riferite a dati definiti *particolari.*

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. Esso deve riportare: la motivazione delle riprese (sicurezza, organizzazione, sicurezza sul lavoro); riportare il titolare/responsabile del trattamento (nome azienda/vigilanza); se presente, i dati di contatto del DPO; un elenco sintetico dei diritti dell'interessato; i tempi di conservazione; il codice Qr, che rimanda ad un sito web con l'informativa completa (secondo le linee guida dovrebbe contenente anche una mappa del posizionamento delle telecamere) o le istruzioni per richiederla e l'indicazione delle modalità per avere altre informazioni non presenti sul cartello (vedi fig 1).

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 superiori, è necessario richiedere l'autorizzazione all'ufficio del Garante della privacy.

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.

Fig.1 Esempio di cartello da apporre in prossimità del raggio d'azione delle telecamere

LOGO AZIENDALE (facoltativo)
QR CODE (consigliato)
(con collegamento alla pagina web contenente l'informativa completa)

AREA VIDEOSORVEGLIATA

Il Titolare/Responsabile del trattamento è ……
Via …… Città …… ( ),
Pec……
Responsabile della Protezione dei Dati…….
email ……..

L'area è sottoposta a videosorveglianza per motivi di:

- ☐ **tutela del patrimonio**
- ☐ **sicurezza delle persone/controllo accessi**
- ☐ **organizzazione del lavoro**
- ☐ **sicurezza sul lavoro**

I filmati vengono conservati per n° …….. giorni.

La base giuridica del trattamento è rappresentata dal legittimo interesse (art.6 del Gdpr).
I soggetti interessati possono godere dei diritti previsti, sui propri dati. I principali, per questo trattamento sono: l'accesso, la cancellazione, l'opposizione al trattamento, l'oblio.

Per maggiori informazioni, è possibile consultare l'informativa completa (art.13 del Gdpr) attraverso una delle seguenti modalità: presso i nostri uffici; sul nostro sito web; richiedendola via email all'indirizzo …… o inquadrando il QRCode soprastante.

Art. 13 del Codice in materia di protezione dei dati personali D.Lgs. 101/2018 e del Regolamento UE 2016/679 (GDPR)

I geo localizzatori gps nei veicoli aziendali

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.

la diffusione dei dati personali nei paesi extra UE

Lo svolgimento di alcune attività aziendali potrebbe prevedere l'esigenza di diffondere i dati personali di clienti o collaboratori in paesi non appartenenti all'Unione Europea.
Diffondere i dati verso paesi che non aderiscono alla normativa europea sulla privacy è consentito solo a determinate condizioni:

1) è indispensabile all'esecuzione del contratto di fornitura o il cliente ha espresso il consenso esplicito;

2) il paese destinatario dei dati è stato iscritto all'elenco dei paesi con condizioni di adeguatezza (elenco presente sul sito del Garante della privacy) o esistono accordi bilaterali tra paese mittente e paese destinatario o l'azienda destinataria è riconosciuta come azienda affidabile e gode di condizione di adeguatezza o esistono condizioni vincolanti di contratto tra azienda mittente e azienda destinataria. In quest'ultimo caso, deve sussistere un vincolo contrattuale che garantisca il soggetto interessato (colui al quale i dati si riferiscono) all'esercizio dei propri diritti in tema di privacy, anche con il ricorso al sistema giudiziario, se necessario.
Inoltre, visto che il primo responsabile, in caso di violazione, resta sempre il titolare dei trattamenti, quest'ultimo dovrebbe accertarsi, con tutti i mezzi possibili, che il soggetto straniero segua delle comprovate misure di tutela e sicurezza dei dati personali trattati.

La diffusione di dati transfrontaliera deve essere indicata:

- nell'*informativa* sul trattamento dei dati;
- nel *registro dei trattamenti*.

Deve essere valutato l'impatto, tramite lo strumento della *valutazione di impatto privacy* se il trattamento riguarda dati *particolari* e/o se esso viene effettuato su larga scala, cioè su un numero elevato di soggetti.

Atti di nomina e ruoli

Il *titolare dei trattamenti*, cioè l'entità giuridica che determina il trattamento e la sua finalità trasferisce i dati, per esempio, dei suoi clienti o dei suoi dipendenti, ad una entità transfrontaliera privata (azienda). Quest'ultima diventa un *responsabile esterno* del trattamento. La responsabilità andrebbe definita tramite un apposito atto giuridico (vedi il modello riportato nel capitolo "Adeguare la propria impresa in dieci mosse"), anche se generalmente, per motivi organizzativi, player, come Microsoft, Apple, etc., si "autonominano" responsabili del trattamento, indicandolo nei moduli contrattuali.
Ricordiamo che, comunque, il titolare dei trattamenti resta il primo responsabile che ha il dovere di rendere conto al soggetto interessato, che dovesse subire danni a seguito di violazioni e utilizzi illeciti dei dati.

Il telelavoro

L'obiettivo di questo capitolo è quello di consentire all'azienda di approcciare il telelavoro o smart working, come viene comunemente definito, acquisendo alcune informazioni di base, necessarie per potersi orientare nel vasto panorama tecnologico e normativo, riferito al tema della privacy e della sicurezza delle informazioni e dei dati trattati.
Non abbiamo la pretesa di esaurire il tema del telelavoro in poche righe, ma siamo certi di poter fornire alcune idee e alcune importanti linee guida che il datore di lavoro può scegliere di adottare per rendere più sicura l'attività lavorativa da remoto dei propri collaboratori.

1) L'implementazione del telelavoro in azienda.

Il telelavoro o *Smart working*, traduzione letterale, "lavoro intelligente", definisce lo svolgimento dell'attività lavorativa, da parte dei collaboratori, presso un luogo remoto, diverso dalla sede operativa dell'impresa, generalmente coincidente con la propria abitazione.
Ci siamo abituati a sentire questo termine nel periodo della chiusura forzata degli uffici (lockdown) durante il periodo di lotta alla pandemia dell'ormai tristemente noto virus Covid – 19, quando il lavoro svolto da casa rappresentava l'unica alternativa per molte aziende per continuare la propria attività.
Tuttavia, lo smart working era già una prospettiva per molte imprese e rappresentava, anche prima del periodo di chiusura a seguito della pandemia, un'opportunità per ottimizzare tempi e costi della propria attività. Noi pensiamo che lo smart working, in quel periodo, forzato, possa diventare in futuro un modello di business sostenibile e auspicabile per molte imprese.
Gli elementi di base che devono essere presenti presso la sede remota del collaboratore per la gestione dell'attività di smart working sono i seguenti:

- linea di collegamento (Internet – Vpn – Cdn);

- personal computer (laptop o desktop);

- smartphone;

- eventuale stampante;

- eventuale hard disk o Nas per il back up;

- applicazioni software per l'attività (navigazione web; posta elettronica; app specifiche per l'attività lavorativa) e la sicurezza (antivirus-antiransomware-firewall);

- applicazione o dispositivo per la timbratura virtuale.

Analizzeremo, di seguito, diversi modelli organizzativi di smart working con le loro peculiarità e caratteristiche; come dovrebbero essere concepiti e organizzati, qual è il loro impatto sulla privacy delle persone rispetto alla normativa vigente e quali sono i documenti e le misure di sicurezza da implementare.

2. Smart working con utilizzo esclusivo di dispositivi aziendali

Si tratta della situazione ottimale, cioè del tipo di organizzazione alla quale bisognerebbe auspicare: computer, software utilizzato, linea di collegamento con l'infrastruttura informatica aziendale (VPN, Virtual Private Network) appartiene al datore di lavoro.

2.a Linea di collegamento (VPN)

Il datore di lavoro, si occupa di fornire tutti i dispositivi necessari, a partire dal collegamento VPN, cioè una linea privata virtuale che connette, utilizzando i comuni protocolli Internet, l'abitazione del collaboratore ai server aziendali.

La linea è virtuale perché, al contrario di una linea LAN, utilizzata all'interno dell'azienda o una linea CDN, conosciuta anche come "linea dedicata", che utilizza un collegamento fisico tra i dispositivi, la VPN utilizza la rete Internet come "veicolo" di collegamento. Al contrario, però, di un normale collegamento standard effettuato tramite Internet, che presenta un basso livello di sicurezza per via della sua connotazione pubblica, la VPN garantisce la privatezza dei dati trasmessi grazie anche alla crittografia applicata ai collegamenti e all'obbligo di autenticazione per il suo utilizzo. Per usare una metafora, per spiegare meglio il concetto, è come se percorressimo una via su un mezzo pubblico, insieme a tante persone che possono ascoltare i nostri discorsi o su un'auto privata, dove sale solo chi vogliamo noi. La via è sempre la stessa (Internet) ma il mezzo consente un utilizzo più ristretto e sicuro.

Riepiloghiamo i vantaggi del collegamento via VPN:

- economicità rispetto a linee dedicate;

- qualità e sicurezza dei collegamenti;

- flessibilità rispetto a cambiamenti delle reti;

- possibilità di connettersi a più sedi fisiche dell'azienda, dislocate in qualsiasi paese.

Quando parliamo di sicurezza, ci riferiamo alla sicurezza rispetto alla riservatezza e all'integrità dei dati, dato che la crittografia e la "schermatura" dell'indirizzo IP (Internet Protocol, l'indirizzo che consente di rintracciare tutti i dispositivi connessi in rete) consentono una maggior protezione da attacchi esterni effettuati da hacker, simulando un collegamento interno all'azienda.
Sul mercato esistono molti provider che possono fornire questo tipo di tecnologia. L'attivazione è rapida e semplice e non necessità di installazioni fisiche. È tuttavia necessario configurare specificamente i firewall e i router degli apparati utilizzati.
La VPN è attivabile anche per collegamenti da smartphone, ma attenzione alle insidie presenti sul mercato: tramite Google Play Store sono state diffuse alcune app, in particolare per sistemi Android (sistemi operativi utilizzati da Samsung, Huawei, etc., non da Apple, che utilizza IOS), che nascondendo importanti vulnerabilità, hanno esposto milioni di utenti e di dati agli attacchi degli hacker.

Di seguito, alcune app pericolose segnalate dagli esperti di sicurezza informatica:

- Tap VPN Free VPN;

- Best Ultimate VPN – Fastest Secure Unlimited VPN;

- Korea VPN – Plugin for OpenVpn;

- Wuma VPN-PRO;

- Super VPN 2019 USA.

Ce ne sono molte altre e alcuni elenchi sono ritrovabili nel WEB. Di regola, è sempre bene diffidare dei servizi gratuiti e utilizzare prodotti commercializzati da provider conosciuti.

2.b Personal Computer, Smartphone e sicurezza informatica

Il tema della sicurezza informatica deve essere necessariamente affrontato, non soltanto quando si implementa un'attività di telelavoro, tuttavia, nel caso specifico, diventa un elemento ancora più determinante. Infatti spesso ci troviamo di fronte a situazioni precarie, collegamenti effettuati in emergenza e spesso senza la possibilità di seguire pedissequamente tutte le buone pratiche al fine di minimizzare i rischi di perdita di riservatezza, disponibilità e integrità dei dati.

Il telelavoro può essere effettuato tramite laptop, pc e smartphone. Tutti i dispositivi che trattano e conservano dati devono prevedere le installazioni e le procedure di base atte a garantire la massima sicurezza.

Per le istruzioni di base, rimandiamo al paragrafo 9 del manuale, "Le basi della sicurezza fisica e informatica"

Anche se viene utilizzata una linea VPN per il collegamento all'azienda, la garanzia alla protezione dei dati non è mai totale, anche perché all'interno della rete aziendale potrebbero esserci molti punti "deboli" di potenziale accesso da parte di malintenzionati. Inoltre, anche il semplice inserimento di una chiavetta usb infetta o l'apertura di un sito/file infetto potrebbe inficiare tutto il sistema di sicurezza aziendale.

2.c Dispositivo di back up

Sicuramente, un dispositivo fondamentale, soprattutto se il lavoro svolto in remoto richiede un'elaborazione di dati effettuata in locale, è quello di back up. Sarebbe sempre auspicabile che questo avvenisse nel momento del collegamento ai server aziendali in modo centralizzato e magari duplicato in un sistema di cloud sicuro. In ogni caso, un back up del lavoro svolto, anche semplicemente utilizzando un hard disk esterno, piuttosto che un Nas protetto da password, è sempre consigliato.

2.d Policy e contratto di utilizzo del dispositivo

I dispositivi aziendali utilizzati devono essere inseriti nell'elenco degli "asset" impiegati per il trattamento dei dati personali e correlati al soggetto che li utilizzerà.
A completamento della documentazione, non solo ai fini della privacy, ma anche per definire, nel contesto di un protocollo organizzativo aziendale, l'utilizzo e la collocazione dei beni strumentali dell'impresa, sarà necessario redigere un contratto di utilizzo, nel quale viene indicato il dispositivo, assegnato al collaboratore, completo di: data di consegna, durata dell'assegnazioni, motivazione, condizioni e raccomandazioni per il suo utilizzo.
Tutte le indicazioni inerenti l'utilizzo nel rispetto delle buone pratiche di sicurezza, accennate nel precedente paragrafo, sarebbe consigliabile inserirle in una "policy per l'utilizzo della strumentazione" fornita insieme al contratto di utilizzo. Policy e contratto devono essere redatte in doppia copia. Una copia resterà al collaboratore e l'altra, firmata (la policy, firmata per presa visione) sarà conservata in azienda in un apposito faldone, classificato con data di emissione.

3. Smart working tramite l'utilizzo dei dispositivi privati

La fornitura al collaboratore dei beni strumentali per lo svolgimento dell'attività in smart working consente all'azienda di mantenere un più alto controllo relativamente alle modalità di utilizzo del dispositivo, ai software installati e all'applicazione di tutte le buone pratiche auspicabili per la tutela dei dati trattati, in conformità alla normativa vigente.
Situazioni emergenziali, quale quella sanitaria tutt'ora in corso, tuttavia, potrebbero far divenire necessarie soluzioni alternative, pur non ottimali, per poter continuare ad operare.
Si fa riferimento al caso in cui, onde svolgere l'attività lavorativa da remoto, il dipendente/collaboratore sia autorizzato ad utilizzare propri dispositivi, trattando dati di cui l'azienda è titolare e, magari, anche connettendosi al sistema di elaborazione dati (gestionali, server ecc.) dell'azienda medesima.
A seconda delle modalità con cui viene eseguito il trattamento e della tipologia di dati trattati, tali condizioni non ottimali possono anche risultare accettabili, se non altro in considerazione della temporaneità e della natura emergenziale delle circostanze.
In linea di massima, tuttavia, è auspicabile che, in particolare, alcune categorie di dati, come quelli sanitari e giudiziari, non vengano trattati se non in presenza di un'infrastruttura informatica in grado di garantirne la massima protezione e tutela.
Pertanto, la prima valutazione da fare, per stabilire la correttezza o meno delle modalità con cui viene eseguito il trattamento, è relativa al rischio prevedibile, per i diritti e le libertà fondamentali dei soggetti interessati, nel caso in cui si verificasse una violazione dei dati.
Nel caso di utilizzo dei dispositivi privati, onde mitigare la rischiosità connessa alla modalità del trattamento così eseguito, si può agire condividendo una policy che raccomandi un comportamento del collaboratore in linea con le indicazioni aziendali rispetto alla riservatezza e all'uso lecito dei dati, oltre che alla sicurezza in tema di strumentazione informatica.
La policy deve rappresentare una linea guida che renda cosciente il collaboratore dei rischi che si corrono omettendo di mettere in atto determinate precauzioni.
Ricordiamoci, però, che la responsabilità di eventuali violazioni ricade sempre sul titolare dei trattamenti, cioè l'azienda, la quale potrebbe rivalersi sul collaboratore solo in caso di dolo da parte di quest'ultimo.

Dal punto di vista tecnico, in considerazione del fatto che, vista la rischiosità del trattamento, la possibilità di minacce provenienti dall'esterno è maggiore, l'azienda, al suo interno, deve operare in modo più attento e sistematico per garantire la sicurezza dei suoi sistemi.
È consigliabile, in questo caso in particolare, effettuare frequenti analisi delle vulnerabilità, test con gli antivirus, cambi di password e, se possibile, mantenere monitorato l'intero sistema anche con sistemi di *remote monitoring system,* sistemi di controllo continuo del sistema informatico, utilizzati da molte società di assistenza informatica. In questo modo, segnali di disfunzione di sistema o anomalie nel funzionamento della rete aziendale vengono tempestivamente rilevati da chi è in grado di mettere in atto dei correttivi per il contenimento o la prevenzione di danni ingenti.

In sintesi, alla domanda che spesso ci perviene, se sia possibile impostare lo smart working autorizzando il collaboratore ad utilizzare il proprio pc, si può dare risposta positiva se il rischio derivante da eventuali violazioni non risulta eccessivo e accompagnando questa valutazione all'adozione di una policy e delle misure tecniche sopra descritte.

Due articoli della normativa europea (GDPR), rispettivamente il 24 e il 32, definiscono la responsabilità del titolare dei trattamenti nel mettere in atto tutte le misure idonee per la protezione dei dati, quindi il margine di operatività è ampio, a patto che le misure intraprese siano proporzionate al rischio affrontato e alla dimensione dell'impresa. È quindi indispensabile redigere un'accurata analisi dei rischi e degli impatti, prevedendo di implementare tutte le adeguate misure di sicurezza al fine di mitigare le vulnerabilità rilevate. Non dobbiamo dimenticare che un'eventuale infezione informatica o una indesiderata intrusione da parte di hacker può essere agevolata o veicolata proprio attraverso i collegamenti esterni con dispositivi vulnerabili.

4. Desktop remoto

Una possibile valida soluzione intermedia è rappresentata dall'utilizzo di un software che consenta, da remoto, di accedere in modo virtuale alla propria postazione in ufficio.
Questa soluzione è consigliabile se sul pc o sul server aziendale sono presenti applicazioni complesse difficilmente trasportabili su laptop aziendale oppure se il collaboratore deve utilizzare un suo pc o laptop privato ma ha necessità di accedere a funzioni in locale presenti solamente sul pc in azienda.
Alcuni dei software più diffusi sono: Team Viewer, Microsoft RDP, VNC, etc. Tuttavia, il tema della sicurezza, diventa molto rilevante visto che questi sistemi potrebbero essere a rischio di una potenziale intrusione in rete, da parte di malintenzionati. Inoltre, potrebbe essere complicato e costoso rendere compatibili dei sistemi Machintosh con dei dispositivi operanti con Windows.
Esistono soluzioni alternative, multitasking, in grado di dialogare con ambienti misti Mac e Windows che consentono di connettersi via Internet in modo molto sicuro alla postazione in azienda, dove il datore di lavoro può decidere se l'accesso debba avvenire a tutte le applicazioni presenti o solo ad una parte di esse.

5. La privacy del dipendente e la timbratura virtuale

Il lavoro in "smart working" non esime, naturalmente, il dipendente dall'effettuare la consueta timbratura.
Per effettuare la timbratura a distanza, oggi è possibile utilizzare degli appositi dispositivi o delle app facilmente scaricabili e utilizzabili dal proprio smartphone, se servisse, anche abbinati ad un sistema di geolocalizzazione GPS. **Nel caso in cui si utilizzasse la geolocalizzazione, è necessario redigere una valutazione d'impatto privacy**, **per** definire e mitigare i potenziali rischi di abusi ed illeciti ed **utilizzare il sistema di localizzazione rispettando i principi del GDPR** che prevedono la minimizzazione dei dati raccolti, i tempi del trattamento ed il loro utilizzo.

6. Implementazione della documentazione privacy per il telelavoro

In sintesi, elenchiamo di seguito la documentazione di cui, a seconda della casistica aziendale, è necessario o opportuno dotarsi, per la conformità alla vigente normativa privacy.

a) Informativa dipendenti.

Da integrarsi nell'ipotesi di in cui la timbratura venga effettuata da remoto tramite app o appositi dispositivi, con l'indicazione della stessa circostanza di acquisizione e trattamento del dato da remoto nonché dell'eventuale utilizzo dei dati di geolocalizzazione con specificazione delle finalità che legittimano il trattamento e che ne dettano i limiti, ai sensi dalle vigenti normative in materia di privacy e di diritto del lavoro.

b) Inserimento nel registro dei trattamenti degli ulteriori dati oggetto di trattamento (vedi l'ipotesi della geolocalizzazione) e delle misure di sicurezza implementate per garantire la sicurezza dei dati oggetto di trattamento in smart working (art. 30 del GDPR).

c) Inserimento nell'elenco degli "asset" ("dispositivi di trattamento dati") di tutti i dispositivi eventualmente non ancora censiti, come pc, laptop, smartphone, hard disk esterni, nas, etc.

d) Aggiornamento delle analisi dei rischi relative a ciascun trattamento, indicando l'ipotesi di trattamento dei dati da parte del dipendente/collaboratore in smart working e le misure di sicurezza implementate a tutela dei dati medesimi.

e) Redazione dell'analisi di impatto (DPIA – art.35 del GDPR) nel caso in cui, a titolo di esempio, si trattino i dati di geo-localizzazione ovvero, per il trattamento, si utilizzino strumenti automatizzati (si veda il caso della rilevazione della temperatura corporea per l'accesso in azienda con strumenti automatizzati).

f) Redazione di un contratto di comodato d'uso per l'assegnazione al dipendente/collaboratore dei dispositivi che il medesimo è autorizzato a recare presso il proprio domicilio ovvero, in ogni caso, al di fuori dei locali aziendali.

g) Redazione di una policy per l'utilizzo dei dispositivi e della rete, specifica per l'ipotesi dello smart working con dispositivi del dipendente/collaboratore.

h) Redazione di una policy per il corretto utilizzo dei dispositivi informatici, della rete, delle caselle di posta elettronica nonché più in generale, dei dati trattati.

7. Proteggersi con una polizza assicurativa

Una buona configurazione della propria infrastruttura informatica, unita ad una corretta formazione degli addetti e alla corretta applicazione di tutte le buone pratiche auspicabili, rappresenta un ottimo punto di partenza, che certamente diminuisce i rischi e i danni causati dagli attacchi informatici.
Ciò, tuttavia e come noto, purtroppo non garantisce al 100% l'integrità e l'inviolabilità dei sistemi e dei dati in essi contenuti.
Le conseguenze di una violazione informatica si ripercuotono significativamente sull'attività aziendale, causando fermi produzione, truffe, danni reputazionali, danni fisici ai sistemi e disservizi che potrebbero generare legittime pretese risarcitorie da parte di terzi, cali di fatturato e di liquidità, sanzioni e costi per il ripristino dei sistemi.

Oggi è possibile azzerare o perlomeno ridurre drasticamente i danni che potrebbero essere causati da un cyber attacco e il suo impatto negativo sull'attività d'impresa, per mezzo di una valida copertura assicurativa.
È indispensabile, tuttavia, scegliere il miglior partner assicurativo, che sia in grado, sulla scorta della sua specifica competenza in un settore peculiare quale quello del cyber risk, di consigliare al meglio l'azienda, proponendo la polizza più adatta, selezionata sulla base della dimensione aziendale, del settore merceologico, dell'organizzazione e della tecnologia adottata.

Ispezioni e sanzioni.

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.

Il Garante, generalmente, definisce i criteri su dove effettuare ispezioni specifiche, tramite il Nucleo Privacy della Guardia di Finanza, ma segnalazioni al suo ufficio possono giungere dalle forze dell'ordine, in generale, come Polizia Amministrativa; Ispettorato del Lavoro; Nuclei Territoriali della Guardia di Finanza; etc. e persino da comuni cittadini, che possono organizzarsi o effettuare anche singole segnalazioni utilizzando i comuni mezzi di contatto, seguendo le istruzioni presenti sul suo portale web.

Alcune specifiche dell'applicazione del GDPR nei diversi settori merceologici

Abbiamo affrontato, seppur in modo schematico, le nozioni di base e i principali steps di base per la messa in conformità dell'impresa alle vigenti normative sulla privacy e sulla protezione dei dati.
Le regole di base sono da intendersi valide per tutte le situazioni, tuttavia, come potrete ben immaginare, l'organizzazione aziendale, a seconda dell'area merceologica nella quale opera e/o in base a come è strutturata, può avere delle peculiarità che incidono, anche in modo considerevole, sulle misure da applicare; sui ruoli ricoperti e sugli adempimenti da espletare.

1) Il settore sanitario

a) Medicina di base; medicina del lavoro; medicina preventiva – Liberi professionisti

L'insieme dei dati sulla salute, attribuibile a specifici individui, rappresenta certamente un'area caratterizzata da un contenuto informativo molto intimo e delicato che, in caso di violazione o di utilizzo non attento o illegittimo, può generare una minaccia rilevante per i diritti e le libertà fondamentali dei soggetti interessati. I rischi si potrebbero riscontrare, oltre che nell'ambito della salute personale, nella reputazione dell'individuo; nel riscontro di situazioni discriminanti e di svantaggio a livello sociale.
Il personale appartenente alle categorie delle professioni sanitarie è sottoposto a regole derivanti dalla deontologia professionale medica che già definisce in parte i comportamenti da tenere nell'ambito della tutela dei dati personali. A medici, infermieri e a tutto il personale sanitario, nell'ambito della medicina preventiva; medicina di base e medicina del lavoro, è stato riconosciuto, dal Garante, il ruolo di "titolare autonomo dei trattamenti" dato che, in virtù della loro professionalità, sono gli unici a poter definire quali dati sanitari è utile trattare per le finalità di salute pubblica.

Schematizzando ruoli, adempimenti e regole di base:

- ruolo del medico libero professionista/azienda sanitaria: titolare autonomo dei trattamenti;

- ruolo dell'eventuale assistente/personale di segreteria: autorizzati ai trattamenti;

- ruolo società di manutenzione elettromedicali (se memorizzano dati), dispositivi informatici e impianto di videosorveglianza; consulente del lavoro; società di elaborazione contabile; società esterna di gestione appuntamenti; etc.: responsabile esterno dei trattamenti;

- redazione del Registro dei Trattamenti titolari e di tutta la documentazione di base privacy (analisi rischi; informative; nomine; etc.);

- consenso del paziente: non serve se non si redige il Fascicolo Sanitario Elettronico e/o il Dossier Sanitario. Nel caso di redazione di questi ultimi, serve un consenso specifico (la norma risale al 2012 ed è in corso una valutazione sulla sua applicabilità futura). Il paziente può opporsi al trattamento, anche parziale, dei dati inseriti nell' Fse o nel Dossier Sanitario; serve il consenso per l'utilizzo dei dati per finalità promozionali (ad esempio, la carta fedeltà delle farmacie o newsletter), per l'utilizzo di dispositivi elettromedicali personali portatili quando le finalità non sono direttamente collegate allo stato di salute del soggetto (ad esempio, finalità commerciali, statistiche non anonimizzate, etc.);

- in caso di consulto con altri medici, questi diventano contitolari dei trattamenti;

- dpo (responsabile della protezione dei dati). Non sono tenuti a nominarlo i liberi professionisti e i piccoli studi, mentre, al contrario, lo sono, le cliniche, grossi studi (medicina di gruppo), laboratori di analisi, grosse imprese di medicina del lavoro e, in generale, chi effettua trattamenti massivi di dati;

- non è possibile consegnare ricette; prescrizioni e referti medici a persone diverse dall'interessato, a meno che non ci sia una delega scritta del paziente. Il documento deve essere all'interno di una busta sigillata. Lo stesso vale per le ricette consegnate all'incaricato della farmacia. Sarebbe da evitare anche la prassi di lasciare le ricette mediche incustodite a disposizione nella sala d'attesa, anche se in busta chiusa;

- è da porre una particolare attenzione a tutte le misure di sicurezza, fisica e informatica, da applicare agli strumenti di trattamento di dati sanitari;

- è da valutare l'esigenza o meno di analisi di impatto, sulla base dell'attività svolta e degli strumenti utilizzati, come ad esempio, dispositivi di trattamento automatizzato di dati o attività con categorie di persone particolarmente vulnerabili;

- I dati utilizzati in forma anonima, cioè con l'impossibilità materiale di risalire all'identità del soggetto interessato (diversi quindi dai dati "pseudonimizzati"), trattati per finalità statistiche o di ricerca, non necessitano di consenso e non sono sottoposti alle regole del GDPR.

b) Medicina di base; medicina del lavoro; medicina preventiva – Aziende o liberi professionisti associati

Restano valide le regole di base elencate per i liberi professionisti con le seguenti eccezioni:

- ruolo: l'azienda di medicina del lavoro è responsabile esterno, nei confronti del datore di lavoro del dipendente, mentre, il singolo medico professionista è titolare autonomo del trattamento;

- il dpo deve essere nominato se il trattamento di dati è massivo.

Tra le regole comuni da applicare alle due tipologie professionali, c'è la corretta gestione della consegna dei referti on line:

questa prevede tutta una serie di modalità sulle quali si era già espresso il Garante nel 2009 e con le linee guida a seguito del decreto 101/2018.

Vediamo in sintesi quelle principali:

- le modalità di consegna dei referti prevedono il download da un portale web, oppure, l'invìo per e-mail all'interessato;

- l'interessato deve esprimere il consenso esplicito e un'informativa esaustiva;

- applicazione di tutte le misure di sicurezza, come, ad esempio, protocolli di comunicazione sicuri; sistemi idonei di autenticazione; disponibilità del referto per non più di 30gg.; possibilità di cancellazione; spedizione via mail solo in forma di allegato; convalida degli indirizzi mail dei corrispondenti; separazione dei dati amministrativi da quelli sanitari; etc.

- è vietato trasmettere in forma digitale dati genetici o inerenti l'HIV.

2) Le aziende commerciali e di produzione

Ciò che caratterizza l'analisi da effettuare in azienda è l'attenzione da porre ai vari soggetti coinvolti al fine di determinare i ruoli privacy da assegnare e l'impatto della normativa privacy sui vari soggetti, in relazione ai processi applicati.

Iniziamo dai ruoli:

- Titolare dei trattamenti: l'entità "azienda" con estensione della responsabilità al suo legale rappresentante/amministratore o, in alcuni casi, al direttore generale (ente pubblico o multinazionale con branch gestita nell'Ue);

- Autorizzati al trattamento di dati: generalmente tutti i collaboratori che operano negli uffici (commerciale, amministrativo, personale, etc.); alcuni operai, generalmente i capi squadra, dato che spesso trattano dati di contatto dei colleghi per determinare turni e sostituzioni; soci; organo di vigilanza (se presente); agenti monomandatari se utilizzano regolarmente tutte le strutture aziendali; personale anche interinale che tratta dati di clienti, colleghi e fornitori;

- Responsabili esterni: tipicamente, il consulente del lavoro; il commercialista; l'azienda di medicina del lavoro (se è un medico singolo è un titolare autonomo); la società che effettua assistenza software e/o servizi di cloud; agenti mono/plurimandatari che utilizzano in genere mezzi propri di trattamento dati; consulenti di sicurezza del lavoro; consulenti aziendali e formatori che trattano dati dei dipendenti; società di elaborazione dati che trattano dati di clienti o dipendenti; etc.

- Altri destinatari di dati personali: banche e assicurazioni, organizzazioni sindacali, enti pubblici per gli adempimenti correnti, in qualità di titolari autonomi del trattamento.

Regole principali:

- non è possibile mettere in atto processi finalizzati al controllo del dipendente (ad esempio, telecamere puntate sulle postazioni di lavoro);

- non si possono esporre in pubbliche bacheche: dati personali; graduatorie riferite alle performance aziendali; richiami e note di demerito;

- è possibile comunicare, con il consenso, i dati del dipendente alle organizzazioni sindacali;

- le comunicazioni che hanno finalità differenti dall'esecuzione del contratto di fornitura necessitano di consenso esplicito da parte dei destinatari;

- i dati vanno conservati solo per il periodo necessario allo svolgimento di: forniture; contratti di lavoro; adempimenti. I dati che, per legge, devono essere conservati per più tempo (ad esempio, i dati fiscali, per 10 anni) devono essere eliminati dai dispositivi utilizzati nell'operatività quotidiana e conservati in un luogo sicuro e protetto, non consultabile pubblicamente. Non deve esservi accesso, se non per ispezioni, da parte delle autorità, per esigenze di difesa in sede processuale o per altre motivazioni particolari;

- il datore di lavoro non può trattare i dati particolari (salute, idee politiche, etc.) dei dipendenti. L'unico dato relativo alla salute che può trattare (salvo le eccezioni secondo le disposizioni ministeriali nel periodo post Covid-19) è l'idoneità all'attività lavorativa;

- il dpo è necessario se l'azienda ha dimensioni molto rilevanti (non esiste un limite definito, ma potrebbe essere sensato ipotizzare almeno dai 300/400 dipendenti in su) oppure se effettua trattamenti massivi di dati (aziende di servizi energetici, telefonici, etc.);

- i casi più frequenti di necessità di analisi di impatto privacy riguardano la presenza di videosorveglianza, di controlli accessi con dati biometrici (impronte, cornea, etc.), di localizzatori gps sui mezzi aziendali, l'utilizzo di termo scanner utilizzati per rilevare la temperatura corporea (disposizione anti-Covid 19) o trattamenti particolari di dati.

3) Le aziende di servizi e i professionisti

Rispetto alle aziende commerciali e di produzione, le aziende di servizi sono caratterizzate da una percentuale maggiore di collaboratori autorizzati ai trattamenti e spesso dalla necessità di assumere il ruolo doppio di titolari dei trattamenti (nei confronti dei dipendenti, fornitori e clienti) e responsabili esterni. Infatti, nelle aziende di servizi, spesso ci sono organizzazioni che elaborano i dati di terzi forniti dai loro clienti che, assumono, per quei dati il ruolo di titolari del trattamento.

Facciamo qualche esempio pratico:

società di assistenza su software gestionali: accedono a dispositivi con dati di clienti o di dipendenti dei loro clienti, quindi di terzi;

società di consulenza del lavoro: trattano i dati dei dipendenti dei loro clienti, quindi di terzi;

società di elaborazione di dati di marketing: trattano i dati dei clienti dei loro clienti.

In questi 3 esempi si definisce chiaramente il ruolo di responsabile esterno dei trattamenti nei confronti dei terzi e di titolarità del trattamento, nei confronti del cliente. Ecco quindi il doppio ruolo.

Cosa comporta essere anche responsabili esterni:

- rispondere di mancata applicazione di misure idonee di protezione e tutela dei dati;

- responsabilità sull'utilizzo ed il trattamento dei dati;

- se a propria volta si desidera nominare un responsabile esterno che tratta i dati di terzi (diventa quindi un sub-responsabile), è necessario ottenere il consenso dal titolare dei trattamenti, cioè dal proprio cliente;

- è necessario redigere il registro dei trattamenti doppio: come titolare e come responsabile;

- è necessario indicare sulle informative, inerenti i trattamenti per il titolare dei trattamenti, chi è il titolare dei trattamenti. Può infatti capitare che il soggetto acceda direttamente ai servizi del responsabile.

Tra le aziende di servizi, si annoverano gli studi dei commercialisti e gli avvocati.
Che siano società o studi libero professionali, non cambia molto. In ogni caso, trattano entrambi dati di carattere particolare, quindi che meritano un'attenzione, rispetto alla sicurezza e alla riservatezza, superiore a molti altri titolari e responsabili dei trattamenti.
Ricordiamo la violazione al sistema della pec subita dagli avvocati dell'Ordine degli Avvocati di Roma: i dati sono stati diffusi in rete. A seguito di indagini successive, si è scoperto che molte password erano marcatamente deboli e vulnerabili.
Come per i medici, se non sono strutture molto grandi con trattamenti massivi di migliaia di soggetti, non necessitano del dpo. Come nell'esempio sopraesposto, sia i commercialisti che gli avvocati sono titolari dei trattamenti, nei confronti dei dati personali dei loro clienti e responsabili esterni quando trattano dati di terzi, fornitegli dai clienti stessi.
In particolare, gli avvocati, confermando un parere dell'ANF, sono stati riconosciuti dal Garante titolari autonomi, quando gestiscono in aula una causa utilizzando dati anche di terzi e responsabili esterni quando operano in qualità di consulenti per le imprese.

E' possibile redigere un'unica informativa a patto che contenga tutte le possibili tipologie di trattamento, di categorie di destinatari, etc.

4) Gli amministratori di condominio e le agenzie immobiliari.

Gli amministratori di condominio

Secondo la più recente normativa (legge 220/2012), il condominio è considerato un ente di gestione sprovvisto di personalità giuridica, che agisce per mezzo dell'amministratore, così come confermato da una sentenza della Cassazione, la N° 19663/14. Siamo in presenza, quindi, di un'entità con autonomia patrimoniale imperfetta, che opera tramite gli organi dell'amministratore e dell'assemblea. Tuttavia, la giurisprudenza considera il condominio capace di assumere obblighi e diritti.
La pedissequa applicazione dell'attuale normativa sulla privacy (Reg. EU 679/2016, denominato anche GDPR) vede il condominio come un "titolare del trattamento" dei dati, i condomini come i contitolari del trattamento e l'amministratore come "responsabile esterno" del trattamento, nominato dal condominio stesso. I tecnici, gli artigiani e le aziende che operano nel condominio, a seguito di un incarico definito dall'amministratore, saranno, se trattano i dati personali dei condòmini, "sub responsabili" del trattamento (Art. 28). Talvolta, l'amministratore, assume anche il ruolo di titolare dei trattamenti, in particolare quando tratta i dati dei singoli condòmini per finalità non riferite direttamente all'entità condominiale.
La norma impone che titolari e responsabili esterni del trattamento debbano mettere in atto le misure tecniche e organizzative idonee alla protezione e alla salvaguardia dei dati (Art. 24,32). Tale operazione si rende possibile a seguito di un'analisi dei rischi privacy, che va correttamente documentata. I ruoli di responsabilità e di sub responsabilità devono essere formalizzati con degli appositi atti giuridici, che definiscono anche la modalità e le finalità dei trattamenti svolti. Inoltre, ogni condominio dovrà mantenere aggiornato il registro dei trattamenti (Art. 30), nel caso in cui si dovessero trattare dati particolari, come, per esempio, la situazione di disabilità di un condomino che richiede un lavoro condominiale per l'abbattimento di misure architettoniche. o un impianto di videosorveglianza. In quest'ultimo caso, è necessaria anche la valutazione d'impatto privacy (Art. 35). Inoltre, responsabili, sub responsabili ed eventuali autorizzati al trattamento (per es. i collaboratori dello studio di amministrazione) devono ricevere la formazione sui principi generali della normativa sulla privacy (Art. 29). Gli amministratori di condominio dovranno avere due registri di trattamento: uno come titolari dei trattamenti e uno come responsabili esterni e far avere ai condòmini una guida contenente i principi generali del GDPR e su come utilizzare i dati personali riferiti alla realtà condominiale.
Ricordiamo che il registro dei trattamenti dell'amministratore dovrà riportare tutti i dati, previsti dalla legge, sui trattamenti rispetto a: condomini gestiti, dipendenti di studio, fornitori, eventuale videosorveglianza, etc.
L'amministratore dovrà far pervenire ai condòmini una guida sulla gestione corretta dei dati personali condominiali. Su questo si è espresso anche l'Ente di Normazione Italiano (Uni).
Non è consentito esporre pubblicamente nelle bacheche avvenute presenze o assenze all'assemblea e altri dati e informazioni riguardanti la sfera privata dei condòmini.
Tutti i condòmini hanno il diritto di conoscere la situazione in merito alle eventuali morosità, ma nessuno può diffondere questi dati al di fuori dell'ambito condominiale.

Anche la gestione della videosorveglianza è diversa se è del singolo condomino o condominiale. Solo nel secondo caso si dovranno applicare tutte le regole già esposte nel capitolo specifico del manuale "La videosorveglianza". Tuttavia, anche l'installazione della telecamera privata dovrà seguire alcune regole di base:

1) se installata all'esterno dell'abitazione, il suo raggio d'azione deve essere limitato alla prossimità dell'ingresso di casa, cercando di evitare al massimo la restante area condominiale (pianerottolo, giardino, atrio, etc.);

2) se installata all'esterno dell'abitazione, si dovrà applicare il cartello informativo, riportante tutte le informazioni previste dalla normativa.

Le agenzie immobiliari

Questo tipo di impresa è caratterizzata da alcune specificità di ruolo in quanto è diffusa la prassi di scambiarsi tra network più o meno ufficiali di agenzie le richieste dei clienti. Non ci sono controindicazioni a patto che questa prassi venga indicata nell'informativa e possa essere non accettata dal cliente. Il ruolo privacy delle altre agenzie può essere quello della titolarità autonoma, se il business viene poi finalizzato dalle agenzie destinatarie.

Un altro strumento molto utilizzato è quello dei portali web, all'interno dei quali viene veicolata la richiesta di acquisto, vendita o locazione del cliente. In questo caso, le società che gestiscono i portali diventano responsabili esterni dei trattamenti.

Spesso i primi contatti dei clienti con le agenzie avvengono via web o via telefono. In entrambi i casi è bene esporre (al telefono in modo sintetico) l'informativa per il trattamento dei dati ed l'espressione del consenso (al telefono oralmente, meglio se con registrazione annunciata; nel web, tramite un flag) all'utilizzo del mezzo di contatto (normalmente il cellulare) per l'esecuzione delle attività richieste.

Può diventare fondamentale gestire il processo, secondo i principi della privacy, della visita dell'immobile. Da una parte si dovrà tutelare la sicurezza dell'attuale proprietario/locatore, tracciando l'identità (almeno con la raccolta di nome, cognome e numero di telefono) di chi visita l'immobile, e dall'altra si dovrà tutelare il diritto all'oblio della persona interessata all'immobile, cancellando in tempi ragionevoli i suoi dati dagli archivi.

La sicurezza e la tutela dei dati trattati dalle agenzie è fondamentale, data la tipologia dei dati trattati (reddito; contatti; etc.) e bisognerà evitare assolutamente di rendere accessibili tali dati a terzi, in particolare nelle situazioni in cui il locatore pretende di conoscere la solidità economica dell'aspirante locatario, a meno che quest'ultimo non dia il consenso esplicito e scritto. La soluzione migliore potrebbe essere quella di creare, una volta stabilito il reciproco interesse all'affare, un contatto diretto tra le parti.

Da gestire con attenzione anche la ritenzione dei dati una volta terminato il business. Trascorsi i dovuti tempi tecnici, i dati vanno conservati per le motivazioni e i tempi di legge in luoghi protetti e consultabili solo per fondati motivi o per richieste da parte delle autorità.

5) Hotel e ristoranti

A caratterizzare i pubblici esercizi, quindi il settore horeca, sicuramente la fornitura di servizi a persone fisiche, al di là del loro ruolo di rappresentanza di entità economiche.
In particolare gli hotel, i bed and breakfast e gli affittacamere, si ritrovano a trattare parecchi dati personali. Pensiamo all'accesso ai documenti di identità; alle informazioni relative alle intolleranze alimentari dei clienti; alle situazioni relative le inabilità fisiche che possono richiedere attenzioni particolari (persone in carrozzella; persone non autosufficienti accompagnate; etc.).
Sotto l'aspetto "tecnologico" le criticità maggiori potrebbero derivare da:

- potenziali violazioni sui sistemi informatici e sui portali (dati personali trattati in sede di registrazione, anche in remoto);

- potenziali violazioni della rete wifi pubblica;

- presenza di videosorveglianza;

Per tutti questi aspetti potete consultare il capitolo relativo alla sicurezza informatica.

Ricordiamo due episodi relativi a due famose catene di hotel: il primo si è ritrovato, a causa di un ransomware (infezione software che cripta i dati e chiede un riscatto per la decriptazione), tutte le porte delle camere bloccate; il secondo ha subito una violazione ai dati personali di tutti i clienti che sono stati poi diffusi pubblicamente sulla rete.

Tuttavia, i problemi possono essere non solo tecnologici: pensiamo alla "cattiva abitudine" di registrare i documenti di identità e di lasciarli depositati nel dispenser delle chiavi, alla portata di chiunque. I documenti personali non vanno mai fotocopiati e conservati, ma utilizzati per la raccolta e l'inserimento dei dati nei portali per la registrazione della presenza, come previsto dalla legge, e riconsegnati subito al cliente.
La base giuridica per la raccolta dei dati, prevista dalle norme, non è il consenso esplicito, ma la legge nazionale. Tuttavia il consenso per il trattamento deve essere raccolto per l'utilizzo di tutti quei dati (di contatto, di preferenze alimentari, etc.) che integrano i dati utilizzati per l'esecuzione del contratto di fornitura del servizio. Un consenso al trattamento apposito è sempre necessario per utilizzare mail, telefono o indirizzo a scopo promozionale-pubblicitario.
Se i consensi sono stati raccolti on line non è necessario raccoglierli una seconda volta.

Spesso gli alberghi utilizzano delle strutture locali per agevolare la fruizione di alcuni servizi da parte degli ospiti: noleggio di auto; gite organizzate; etc. Generalmente, queste strutture convenzionate si possono considerare titolari autonomi dei trattamenti, a meno che, il servizio non sia pubblicizzato e venduto direttamente dall'hotel, magari anche col suo brand. In questo caso, tali strutture sono da considerarsi come responsabili esterni dei trattamenti.

I ristoranti che raccolgono i dati fiscali per l'emissione di ricevute o fatture non devono chiedere il consenso. Il consenso, anche in questo caso, è necessario per l'inserimento di mail e telefoni a scopo promozionale o pubblicitario; per tessere fedeltà; etc.

La normativa "post Covid 19" ha imposto una serie regole, probabilmente momentanee, per il controllo della pandemia (valide quando è stato redatto il presente manuale):

- la conservazione del numero di telefono per 14 giorni;

- la misurazione della temperatura corporea.

Queste misure non prevedono il consenso, ma richiedono la presenza dell'informativa; la presenza dei trattamenti nel registro dei trattamenti e la designazione del personale incaricato.

6) Palestre, centri estetici, parrucchieri, tatuatori

La quantità di dati personali particolari, trattati in queste tipologie di attività, è davvero notevole. Infatti, le linee guida del Garante, impongono che venga redatto il registro dei trattamenti anche se l'attività viene svolta in assenza di personale dipendente. Inoltre, l'espressione del consenso privacy deve avvenire sempre, proprio per il fatto che categorie di lavoratori privi di codici deontologici (vedi, ad esempio, il personale esercitante professione medica), sono incaricati di trattare dati sensibili, ora definiti "particolari".
Esempi di dati particolari, nello specifico, possono essere: malformazioni fisiche; allergie e intolleranze a particolari sostanze; patologie della pelle come psoriasi e dermatiti; etc.

Alcuni centri hanno al loro interno strutture che si occupano di massaggi e trattamenti anche di tipo medico, quindi ogni caso deve essere analizzato attentamente.
Spesso, centri massaggi, centri estetici e palestre, come accade negli studi medici, utilizzano personale non assunto, che opera a partita iva, in qualità di ditta individuale, magari per diverse realtà. La differenza del ruolo privacy sta proprio nella tipologia di lavoro:
il dipendente sarà autorizzato ai trattamenti; il collaboratore che opera in qualità di cococo/partita iva per un solo committente sarà nella maggior parte dei casi un autorizzato ai trattamenti; un operatore a partita iva che opera in diverse strutture, con strumenti di trattamento dati propri (pc, tablet; etc.), può essere definito come un responsabile esterno dei trattamenti.

La normativa "post Covid 19" ha imposto una serie regole, probabilmente momentanee, per il controllo della pandemia (valide quando è stato redatto il presente manuale):

- la conservazione dei dati di contatto fino a fine emergenza Covid o fino a 14 giorni successivi la fine dei trattamenti (pensiamo a cicli di più trattamenti estetici, per esempio);

- la misurazione della temperatura corporea.

Queste misure non prevedono il consenso, ma richiedono la presenza dell'informativa; la presenza dei trattamenti nel registro dei trattamenti e la designazione del personale incaricato.
Vista la natura dei dati trattati e spesso il rapporto fiduciario che si instaura tra cliente e operatore, sarebbe opportuno che ogni collaboratore gestisca i dati dei clienti seguiti rispettando il principio della riservatezza dei dati anche nei confronti degli altri operatori.
E' consigliabile la redazione di una policy condivisa contenente tutte le regole per una buona gestione dei dati personali.

7) Ditte individuali, pubblici esercizi e artigiani

E' intuitivo pensare che strutture più piccole abbiano una minor complessità di adeguamento e gestione della privacy, tuttavia ci sono alcuni elementi da tenere in considerazione. Sono infatti molti ormai i pubblici esercizi che fanno uso di carte fedeltà, utilizzo di strumenti di comunicazione promozionale via mail, sms o What's Up e con rimandi su "landing page"; registrazione di dati personali e profilazioni effettuate in base ai gusti personali, la situazione coniugale, l'età, etc.

Ricordiamo che l'utilizzo di tutti questi strumenti e l'utilizzo dei dati con finalità commerciali e promozionali implica l'obbligo di raccogliere un consenso esplicito e specifico espresso per iscritto o tramite flag inviati per mail.

Finalità, diffusione a terzi e qualsiasi altra caratteristica del trattamento deve essere riportata integralmente sull'informativa messa a disposizione del pubblico.

Anche la raccolta ed il trattamento di mail e numeri di telefonini implica la raccolta di un consenso privacy, quindi anche gli artigiani, in particolare chi si reca direttamente presso il domicilio dei clienti per lavori di installazione e manutenzione di impianti, arredi e quant'altro, non è escluso da tale obbligo.

In generale, gli adempimenti che ditte individuali, pubblici esercizi e artigiani devono espletare sono quelli standard già elencati nel capitolo dedicato all'adeguamento dell'impresa al Gdpr, con l'esclusione, per chi non opera coadiuvato da collaboratori e non tratta dati particolari (sensibili) della redazione obbligatoria del registro dei trattamenti.

Tutte le altre regole sono valide: quelle relative alla gestione dei documenti, dei registri se ci sono dipendenti, del rispetto delle finalità dei trattamenti, etc.

Conclusioni

Il presente manuale non ha la pretesa di sciogliere tutti i dubbi e le perplessità che il processo di adeguamento alle normative sulla privacy, data la sua complessità, potrebbe generare. Rappresenta, tuttavia, una guida utile per avere una panoramica e per comprendere almeno i criteri di base applicati nel processo di adeguamento.

Approfondimenti su alcune delle tematiche affrontate si possono trovare nella sezione "news" del sito di Kruzer S.r.l. all'indirizzo: https://www.kruzer.it/it/news ed eventuali quesiti possono essere inoltrati utilizzando il form sempre del sito, all'indirizzo: https://www.kruzer.it/it/contatti

Sicuramente, le situazioni più complesse richiederanno un intervento consulenziale da parte del nostro personale specializzato che, ricordiamo, è formato, in parte, da avvocati e tecnici esperti in tema di privacy e protezione dati.

Abbiamo a tratti accennato alla problematica riguardo la pandemia del Covid -19 che ci sta affiggendo da alcuni mesi. Abbiamo preferito non approfondire l'argomento, vista la variabilità dei provvedimenti governativi sulla scorta dell'evoluzione della situazione, ma fornire semplicemente qualche elemento comunque determinante ai fini della conformità.

Speriamo comunque di aver soddisfatto le vostre esigenze e di avervi trasmesso una piccola parte di know how che può consentirvi di iniziare ad intraprendere, in modo autonomo, il percorso di adeguamento alla normativa privacy vigente.

Buon lavoro.

Daniele Umberto Spano

Bibliografia e fonti:

Federprivacy sito web e varie pubblicazioni, tra cui "Privacy e Regolamento Europeo di Antonio Ciccia Messina e Nicola Bernardi; testo del Reg.EU 679/2016; testo del d.lgs. 101/2018; linee guida del Garante della Privacy italiano; https://www.garanteprivacy.it/; consulenza dello studio legale Bcpb Lex e dell'avv. Francesco Consoli;

Realizzato il 13 luglio 2020