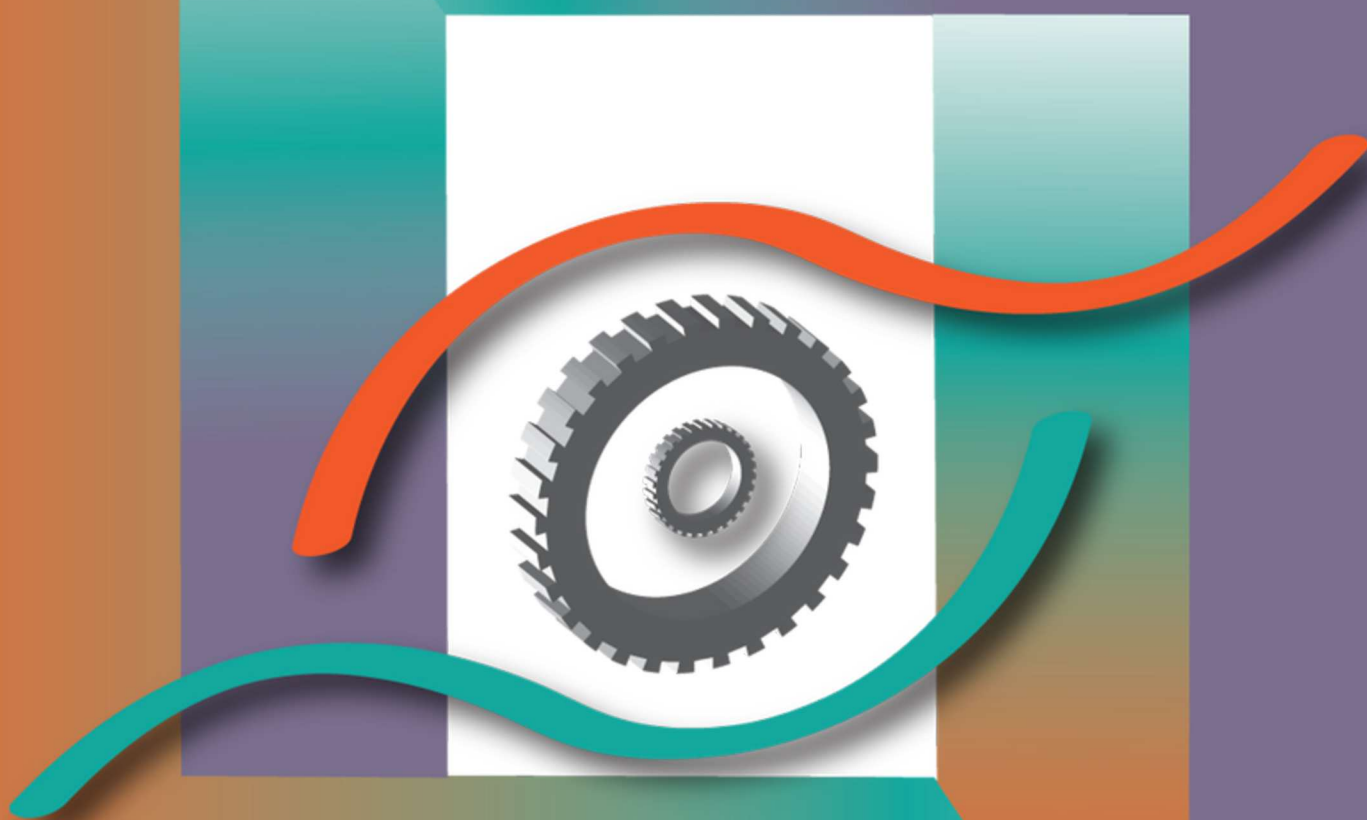


LA TUTELA DEI DATI PERSONALI NEI CONTESTI D'IMPRESA

STRUMENTI E METODI
PER L'APPLICAZIONE DEL GDPR
NELL'ORGANIZZAZIONE
AZIENDALE



DATI PERSONALI: DEFINIZIONE

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.

ESEMPI



NOME, DATI ANAGRAFICI, DATI RELATIVI ALL'UBICAZIONE, CODICI PER L'IDENTIFICAZIONE, C.F., IBAN, CARTA DI CREDITO

ID O IDENTIFICATIVO ON LINE

STATO DI SALUTE, ABITUDINI

IMMAGINE, VOCE, IMPRONTA DIGITALE, DNA

COOKIE

QUALSIASI DATO OGGETTIVO O SOGGETTIVO
CHE SIA RILEVANTE PER IDENTIFICARLO

Per un approfondimento sul concetto di dato personale si veda il parere n. 4/2007 del Gruppo di lavoro ex art. 29.

TRATTAMENTO DI DATI PERSONALI: DEFINIZIONE

Art. 4 del GDPR

«TRATTAMENTO» DEI DATI

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

I PUNTI PRINCIPALI DEL GDPR

BASE GIURIDICA (ART. 6)

Rappresenta il fondamento giuridico che legittima il lecito trattamento dei dati personali. Il legislatore europeo individua quali basi giuridiche per il trattamento dei dati personali: (a) Consenso dell'interessato, (b) Esecuzione di un contratto con l'interessato o di misure precontrattuali a richiesta dello stesso, (c) Obbligo di legge, (d) Salvaguardia interessi vitali, (e) Compiti di interesse pubblico o connessi a esercizio pubblici poteri, (f) Legittimo interesse, a meno che non prevalgano i diritti e le libertà degli interessati

REGISTRO DEI TRATTAMENTI (ART. 30)

Documento essenziale per consentire la mappatura dei trattamenti, del livello di sicurezza applicato e per permettere la verifica anche da parte di terzi circa la sussistenza dei requisiti richiesti dalla normativa (connesso al principio di accountability)

INFORMATIVA (ARTT. 13-14)

L'interessato ha il diritto di ricevere le informazioni identificative sul Titolare del trattamento e sulle finalità, i mezzi e altre circostanze che riguardano il trattamento dei dati personali allo stesso riferibili

DIRITTI DELL' INTERESSATO (ARTT. 15-22)

ACCOUNTABILITY, PRIVACY BY DESIGN E PRIVACY BY DEFAULT (ARTT. 24-25)

ANALISI DEL RISCHIO E VALUTAZIONE D'IMPATTO (ARTT. 32-35)

DATA BREACH (ARTT. 33-34)

RESPONSABILITÀ SOLIDALE DEL TITOLARE E DEL RESPONSABILE DEL TRATTAMENTO (ART. 82)

RAFFORZAMENTO DELLE SANZIONI PECUNIARIE (ART. 83)

PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI (ART. 5 GDPR)

Come trattare i dati personali?

LICEITÀ, CORRETTEZZA E TRASPARENZA: non solo nella finalità di utilizzo dei dati personali ma anche nella varie fasi del trattamento

FINALITÀ: i dati raccolti per una determinata finalità non potranno essere utilizzati per altri scopi o per finalità incompatibili, in caso di trattamento basato sul consenso dell'interessato

MINIMIZZAZIONE: devono raccogliersi e trattarsi solo i dati e le informazioni necessarie al raggiungimento dello scopo predeterminato. "Minimizzare" si traduce nel ridurre al minimo indispensabile la quantità di dati raccolti, l'estensione del trattamento, il periodo di conservazione e l'accesso agli stessi

ADEGUATEZZA, PERTINENZA, LIMITAZIONE: i dati raccolti devono essere sempre corretti e pertinenti al perseguimento delle finalità dichiarate e non devono risultare eccedenti

ESATTEZZA E AGGIORNAMENTO: i dati personali trattati devono essere sempre aggiornati ed esatti

LIMITAZIONE DELLA CONSERVAZIONE: il tempo di conservazione del dato dev'essere commisurato alla finalità prevista

INTEGRITÀ E RISERVATEZZA: il dato trattato deve essere sempre protetto, sia con misure tecniche che organizzative, per garantire un'adeguata sicurezza e protezione dai rischi di trattamento non autorizzato o illecito e dalla perdita, dalla distruzione o da danni accidentali

I DIRITTI DELL'INTERESSATO

Quali sono i diritti esercitabili dagli interessati a cui i dati personali si riferiscono?

Diritti conoscitivi

**DIRITTO
ALL'INFORMATIVA**
(artt. 13 e 14)

DIRITTO DI ACCESSO
(art. 15)

**DIRITTO ALLA
COMUNICAZIONE
DI UNA VIOLAZIONE
DI DATI**
(art. 34)

Diritti di vigilanza

**DIRITTO DI RETTIFICA
E DI INTEGRAZIONE**
(art. 16)

**DIRITTO DI
CANCELLAZIONE/OBLIO**
(art. 17)

DIRITTO DI LIMITAZIONE
(art. 18)

**DIRITTO ALLA
PORTABILITÀ DEI DATI**
(art. 20)

DIRITTO DI OPPOSIZIONE
(art. 21)

**DIRITTO A NON SUBIRE
DECISIONI BASATE
UNICAMENTE
SU TRATTAMENTI
AUTOMATIZZATI**
(art. 22)

INFORMATIVA

Informare l'interessato: come e quando?

1

L'informativa deve sempre essere fornita all'interessato, quando possibile, prima dell'avvio delle operazioni di trattamento dei dati personali

2

Deve essere breve, completa e facilmente comprensibile. Possono essere usati strumenti idonei a facilitarne la lettura (tabelle, icone, caratteri speciali, ecc.)

3

Deve essere indicato il tempo di conservazione del dato raccolto

4

Se il trattamento si fonda sul consenso, l'espressione del consenso deve essere granulare per ogni finalità di trattamento (non è ammesso un consenso generale)

5

Deve essere indicato il destinatario al quale i dati personali sono trasferiti o comunicati

6

Se i dati personali saranno oggetto di diffusione o profilazione

7

I contatti per l'esercizio dei diritti dell'interessato

I PUNTI PRINCIPALI DEL GDPR

ACCOUNTABILITY

Il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR (art. 24, par. 1), quindi a trattare i dati in modo lecito, corretto e trasparente nei confronti dell'interessato (art. 5 GDPR).

Il GDPR, infatti, non è un libretto di istruzioni puntuali, da seguire pedissequamente, quanto, piuttosto, un insieme di coordinate che servono a guidare il titolare del trattamento nelle attività che comportano una gestione dei dati personali, lasciando che sia lo stesso titolare a prevedere e implementare le misure tecniche e organizzative che ritiene, sulla base delle verifiche effettuate, più efficaci a tutelare i diritti e le libertà degli interessati. In questo modo, il titolare si assume la responsabilità delle misure adottate: è il c.d. principio di accountability previsto all'art. 5, p. 2, GDPR, che impone al titolare del trattamento non solo di adottare misure idonee a proteggere i dati personali trattati, ma anche di essere in grado di documentarle.

PRIVACY BY DESIGN

La protezione dei dati personali inizia dalla progettazione



Quando si sviluppano nuovi prodotti, servizi o processi in azienda devono essere valutati gli impatti che tali attività potranno avere sui dati personali



Pertanto è essenziale condurre un'analisi dei rischi circa le minacce per diritti e libertà degli interessati dei cui dati si trattano, ed eventualmente, all'esito, modificare il progetto

"Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate (...) a integrare nel trattamento le necessarie garanzie" (Art. 25, comma 1, GDPR)."

PRIVACY BY DEFAULT

La protezione dei dati personali per impostazione predefinita



Quando si sviluppano nuovi prodotti, servizi o processi in azienda devono essere trattati solo i dati personali necessari e pertinenti alla finalità prevista



Tale obbligo vale per la quantità dei dati personali raccolti, per la portata del trattamento, per il periodo di conservazione dei dati personali e per l'accessibilità ai dati stessi



In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza che vi sia l'intervento della persona fisica (es. trattamenti automatizzati*)

“Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento” (Art. 25, comma 2, GDPR).

DATA BREACH

Cos'è e come gestire una violazione di 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.

Come agire in caso di Data Breach?

FASE 1

Seguire la procedura aziendale interna, precedentemente adottata e resa nota al personale coinvolto

FASE 2

Riunire le figure interne coinvolte, compreso il DPO (quando nominato)

FASE 3

Mettere in atto misure tecniche e organizzative adeguate a scongiurare il sopraggiungere di rischi elevati per i diritti e le libertà delle persone fisiche

FASE 4

Valutare se ricorra l'obbligo di notifica al Garante (entro 72 ore) e di comunicazione agli interessati nei casi previsti agli artt. 33-34 GDPR

CHI È IL DPO?

DPO - Data Protection Officer (artt. 37 e ss.)

Figura di garanzia per il rispetto della normativa in materia di protezione dei dati nel contesto aziendale

In determinati casi è una figura obbligatoria da nominare

Deve essere in possesso di adeguate qualità professionali, conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati

Rappresenta il punto di contatto tra il Titolare o il Responsabile che lo ha designato e l'Autorità Garante

Deve essere adeguatamente, e per tempo, coinvolto in tutte le questioni in materia di protezione dei dati personali

Deve essere supportato con le risorse necessarie a svolgere i compiti

È indipendente ed autonomo nel ruolo, non riceve istruzioni per quanto riguarda l'esecuzione dei compiti connessi all'esercizio della sua funzione di DPO

Riferisce direttamente al Titolare o al Responsabile che lo ha designato

Può essere contattato dagli interessati (tramite i contatti pubblicati anche sul sito aziendale)

Non deve essere in conflitto di interessi (ossia, non può rivestire ruoli che non ne garantiscano l'indipendenza rispetto al ruolo)

PARTE SPECIALE



LA NORMATIVA E LA SUA APPLICAZIONE: CASI PRATICI E COME AFFRONTARLI

#1 Risorse umane

La tutela dei dati personali delle risorse umane si estende a diversi ambiti:

La fase di valutazione
della candidatura e
l'assunzione

01

La videosorveglianza,
il badge o altri strumenti
di accesso che comportano
il trattamento di dati
personali

02

L'utilizzo di rete, dispositivi
e strumenti aziendali, tra cui
quelli che potrebbero consentire
forme di controllo, monitoraggio
o geolocalizzazione

03

L'accesso e l'uso
alla casella e-mail
aziendale

04

Il datore di lavoro è chiamato a svolgere una serie di adempimenti e analisi dei rischi quando tratta dati personali dei dipendenti. Tra questi, l'informativa e la concreta applicazione dei principi di trattamento, tenendo conto anche della normativa giuslavoristica

LA NORMATIVA E LA SUA APPLICAZIONE: CASI PRATICI E COME AFFRONTARLI

#2 Marketing

Cosa stabilisce il Regolamento Generale sulla protezione dei dati (679/2016)?

L'attività promozionale costituisce un legittimo interesse dell'imprenditore, che deve comunque rispettare le norme sulla protezione dei dati (dall'informativa al diritto di opposizione degli interessati e alle misure di sicurezza), introducendo così in capo ai titolari del trattamento l'obbligo di effettuare un bilanciamento di interessi.

Ne consegue che anche secondo il GDPR per le attività di marketing è indispensabile acquisire il consenso degli interessati (Art. 7 e Considerando 32 e 42).

CONSENSO

Come si acquisisce correttamente?

1

Deve essere raccolto contestualmente al conferimento dell'informativa all'interessato, non prima

2

Deve essere registrato e deve sempre essere dimostrabile

3

Deve sempre distinguersi quando inserito in un contesto dove siano presenti altre questioni (es. sottoscrizione contratti, flag di accettazione per termini e condizioni on line, ecc)

4

Deve essere granulare, ovvero riferibile a singole finalità (non può raccogliersi un unico consenso per diverse finalità)

5

Deve essere revocabile facilmente dall'interessato

LA NORMATIVA E LA SUA APPLICAZIONE: CASI PRATICI E COME AFFRONTARLI

#3 Sito Web Aziendale

Il sito web raccoglie dati personali degli utenti sia forniti volontariamente (es. newsletter, richiesta informazioni, invio CV, ecc) sia indirettamente (cookie)*.

A cosa prestare attenzione:

Rendere
una corretta
e trasparente
informativa (cd.
privacy policy e
cookie policy)

Verificare i servizi
forniti o l'uso di app
di terze parti
per il funzionamento
del sito

Verificare
la correttezza
delle sezioni del sito
web adibite
alla raccolta dei dati
personali (c.d. form)

Verificare l'idoneità
delle misure
di sicurezza tecniche
applicate
al funzionamento
del sito web

**Cos'è un cookie: stringhe di testo che i siti web (cd. Publisher, o "prime parti") visitati dall'utente ovvero siti o web server diversi (cd. "terze parti") posizionano ed archiviano – direttamente, nel caso dei publisher e indirettamente, cioè per il tramite di questi ultimi, nel caso delle "terze parti" - all'interno di un dispositivo terminale nella disponibilità dell'utente medesimo. Cfr. Cons. 30 Re. Eu 679/2016 e Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021.*

PROFILI DI COMPLESSITÀ

Quali elementi rilevano nel contesto di:

SITI WEB, E-MARKETPLACE E TRANSAZIONI ON LINE

Contratti pubblici
(Banner, sponsorizzazioni)

Adeguamento alle normative di tutela
del consumatore (termini di consegna,
clausole abusive, recesso, etc.)

Contratti con PSP (per
le problematiche relative
ai pagamenti e alla sicurezza)

Diritto d'autore e privativa
industriale, tutela
dei marchi on-line

Fatturazione elettronica,
logistica e spedizioni

ISP (Es. contratti di locazione)
spazio web o fruizione piattaforme

Privacy policy (informativa,
cookies, log, trasferimento dati
all'estero)

Contratto di sviluppo
e gestione sito web

Validità delle transazioni
commerciali on-line
e loro archiviazione digitale

I SOGGETTI INTERNI AL CONTESTO AZIENDALE (C.D. AUTORIZZATI AL TRATTAMENTO) NELL'ESERCIZIO DELLE LORO ATTIVITÀ DEVONO:

Essere consapevoli dei rischi

Cooperare con Team Privacy/DPO/Security/Sistemi Informativi/Compliance nell'esecuzione della attività lavorativa

Segnalare qualsiasi anomalia nel processo di trattamento dei dati personali

OGNI QUALVOLTA ESIGENZE AZIENDALI RICHIEDANO IL TRATTAMENTO DI DATI PERSONALI, IL TITOLARE:

Deve verificare la corretta applicazione di tutti gli adempimenti richiesti dalla normativa

In casi di questioni complesse che attengono gli adempimenti deve coinvolgere il DPO (quando nominato)

Deve compiere una valutazione dei rischi che il trattamento possa comportare sui diritti e le libertà degli interessati (a cui i dati sono riferibili)

CONSIGLI FINALI

Quando si trattano dati personali è sempre necessario considerare:

COSA

Tipologia di dati
e trattamenti

PERCHÈ

Base giuridica
e finalità

COME

Attraverso quali strumenti, operazioni
e soggetti

QUANDO

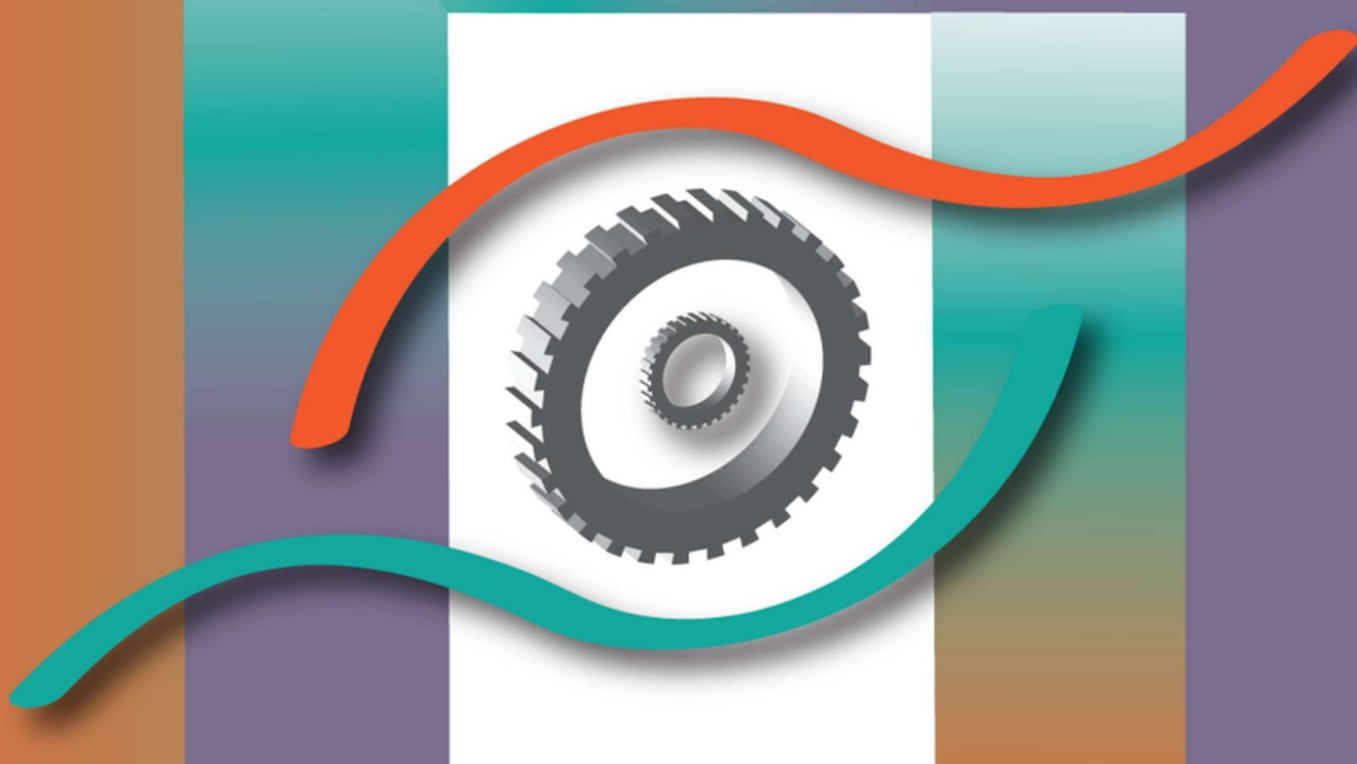
Tempistiche
e conservazione

CHI

Destinatari

DOVE

Luogo di trattamento



Questa infografica è stata realizzata nel mese di **settembre 2022** per **CNA Biella**.

Contenuti a cura di: **Studio Legale Lisi**

Grafica a cura di: **Marcello Moscara**

Impaginazione a cura di: **Digital&Law**