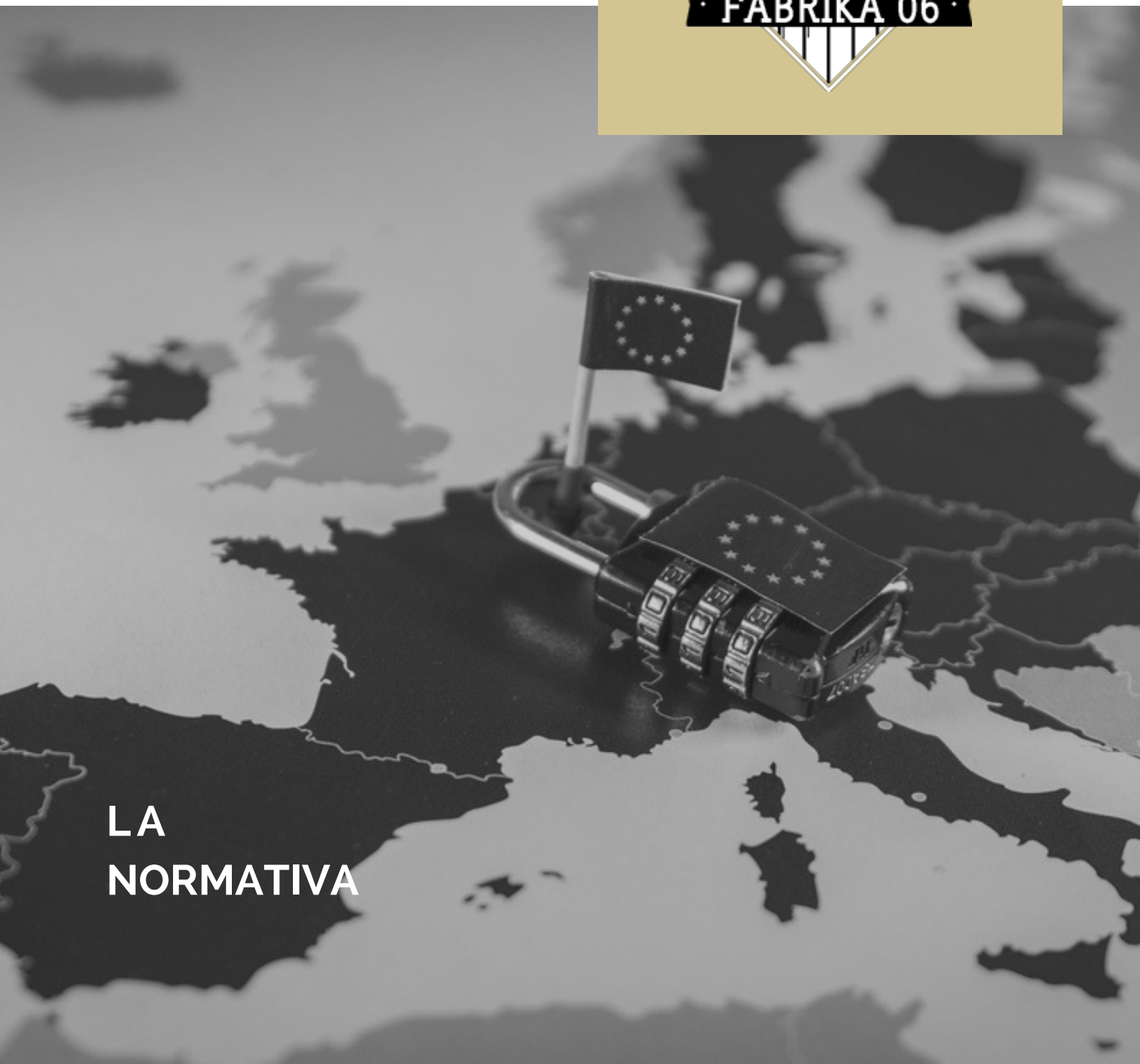
REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI

GDPR

FABRİKA 06



LA NORMATIVA

GDPR

GDPR sta per General Data Protection Regulation (Regolamento generale sulla protezione dei dati personali), ovvero il Regolamento Europeo 2016/679. In estrema sintesi, il GDPR chiarisce come i dati personali debbano essere trattati, incluse le modalità di raccolta, utilizzo, protezione e condivisione. L'obiettivo del GDPR è dunque quello di rafforzare la protezione dei dati per tutte le persone le cui informazioni personali rientrano nel suo campo di applicazione, dando loro il pieno controllo dei propri dati.

Quando si applica

Il GDPR si applica quando:

- la base operativa dell'organizzazione si trova nell'Unione Europea (ciò vale indipendentemente dal fatto che il trattamento abbia luogo nel territorio UE o meno);
- l'organizzazione, seppure non avente sede nell'Unione Europea, offre beni o servizi (anche gratuitamente) a cittadini europei. Può trattarsi di enti pubblici, società private o pubbliche, persone fisiche od organizzazioni senza scopo di lucro;
- l'organizzazione, seppure non avente sede nell'Unione Europea, monitora il comportamento delle persone che vi risiedono, a patto che tale comportamento abbia luogo all'interno del territorio UE.

Un ambito di applicazione così ampio copre in pratica quasi tutte le attività, e pertanto si può concludere che **il GDPR si applica indipendentemente dal fatto che la tua organizzazione si trovi nell'Unione Europea o meno**. Di fatto, questo sondaggio PwC ha evidenziato che il GDPR è una priorità assoluta in materia di protezione dei dati anche per il 92% di tutte le aziende statunitensi intervistate.

Il GDPR è pienamente applicabile a partire dal 25 maggio 2018.

Principali requisiti legali

Definizioni particolari usate nel testo che segue

Con il termine **"utente"** si intende una persona i cui dati personali sono trattati da un titolare del trattamento o da un responsabile del trattamento

GDPR

Con il termine **"titolare del trattamento"** si intende una qualsiasi persona fisica o giuridica coinvolta nella determinazione delle finalità e delle modalità del trattamento dei dati personali degli utenti
Con il termine **"responsabile del trattamento"** si intende una qualsiasi persona fisica o giuridica coinvolta nel trattamento dei dati personali degli utenti per conto del titolare del trattamento

Ad esempio, una società può raccogliere informazioni sugli utenti tramite il proprio sito web e memorizzarle utilizzando un servizio in cloud di terza parte. In questo scenario, la società è il titolare del trattamento dei dati, mentre l'organizzazione che eroga il servizio in cloud è il responsabile del trattamento dei dati.

Basi giuridiche del trattamento

Ai sensi del GDPR, i dati possono essere trattati solo se sussiste almeno una base giuridica del trattamento.

Segue un elenco delle possibili basi giuridiche del trattamento.

- L'utente ha prestato il proprio consenso per una o più specifiche finalità
- Il trattamento dei dati è necessario per l'esecuzione di un contratto al quale l'utente ha aderito,o per intraprendere azioni (su richiesta dell'utente) preliminari alla stipula del contratto
- Il trattamento è necessario per l'adempimento ad un obbligo di legge al quale il titolare del trattamento è soggetto
- Il trattamento è necessario per la tutela di interessi vitali dell'utente o di terzi
- Il trattamento è necessario per l'esecuzione di un'attività di interesse pubblico, o che rientra nell'ambito dei poteri pubblici conferiti al titolare del trattamento
- Il trattamento è necessario per interesse legittimo del titolare del trattamento o di terzi, a meno che non prevalgano gli interessi, i diritti e le libertà dell'utente, in particolare se l'utente è un minore

Consenso

Al fine di effettuare un'attività di trattamento dei dati, l'organizzazione **deve ottenere un consenso inequivocabile** da parte degli utenti.

Nel caso di utenti minori, l'organizzazione è tenuta ad **ottenere un consenso verificabile** da parte di un genitore o tutore del minore, a meno che il servizio offerto non sia di prevenzione o consulenza. L'organizzazione deve altresì compiere sforzi ragionevoli (utilizzando ogni tecnologia disponibile) per verificare che la persona che presta il consenso detenga effettivamente la responsabilità genitoriale del minore.

In generale, al fine di ottenere il consenso al trattamento dei dati, l'organizzazione non può utilizzare termini eccessivamente complicati o indecifrabili. Ciò include il linguaggio giuridico, nonché l'uso di un gergo tecnico superfluo.

Per queste ragioni, **le privacy policy devono essere redatte in modo leggibile**, utilizzando un linguaggio e delle clausole comprensibili, in modo che gli utenti siano pienamente consapevoli di ciò a cui acconsentono e delle conseguenze del loro consenso.

Le organizzazioni devono essere trasparenti in merito alle finalità della raccolta dei dati e **il consenso deve essere "esplicito e libero"**. Ciò significa che la modalità di acquisizione del consenso deve essere inequivocabile e prevedere una chiara azione di "opt-in" (il regolamento vieta espressamente il ricorso a checkbox preselezionate o ad altre metodologie alternative di "opt-out"). Il regolamento sancisce inoltre un **diritto specifico alla revoca del consenso**, che deve essere tanto facile quanto lo è il suo conferimento.

Poiché il consenso ai sensi del GDPR è una questione di primaria importanza, è obbligatorio registrare in modo puntuale i consensi ottenuti affinché l'organizzazione sia in grado di dimostrare che l'utente abbia effettivamente prestato il consenso. L'onere della prova del consenso ricade infatti sul titolare del trattamento, per cui è essenziale conservare queste informazioni in modo estremamente accurato. Le prove del consenso devono includere, in particolare, le seguenti informazioni:

- quando e come il consenso del singolo utente è stato acquisito;
- un riferimento esatto a ciò che è stato detto all'utente in fase di raccolta del consenso, insieme ad un riferimento alle condizioni in essere nel momento in cui il consenso stesso è stato acquisito.

Seguono degli esempi di **archiviazione conforme o non conforme dei consensi**.

Archiviazione non conforme

- Tenere semplicemente un foglio con i nomi degli utenti e un'indicazione sul conferimento o meno del consenso
- Annotare semplicemente la data e l'ora in cui il consenso è stato prestato, associate all'indirizzo IP dell'utente e ad un link alle pagine che ospitano il modulo compilato dall'utente e la privacy policy

Archiviazione conforme

- Conservare una copia del modulo compilato dall'utente, che mostra l'azione intrapresa dallo stesso per prestare il consenso a specifici trattamenti
- Conservare delle informazioni complete che includano un identificativo univoco dell'utente insieme con la data – certificata con marca temporale – in cui il modulo è stato compilato e ad una copia della versione del modulo stesso e dei documenti legali utilizzati nel momento in cui l'utente ha prestato il consenso

Avvertenza sul consenso: *il consenso non è la sola base giuridica per effetto della quale un'organizzazione può trattare i dati degli utenti, ma è solo una delle "Basi Giuridiche" del trattamento. Ai sensi del GDPR, le organizzazioni possono dunque avvalersi anche di altre basi giuridiche del trattamento. Ciò premesso, è bene chiarire che per alcune attività di trattamento dei dati il consenso resta comunque la soluzione migliore, se non l'unica strada percorribile.*

Sempre in materia di consenso, un'altra normativa europea che merita di essere menzionata è la Direttiva ePrivacy (nota anche come Cookie Law). Si tratta infatti di una legge ancora applicabile in quanto non abrogata dal GDPR. In futuro, la Direttiva ePrivacy sarà sostituita dal **Regolamento ePrivacy** che, in quanto tale, lavorerà a fianco del GDPR. Il nuovo Regolamento ePrivacy dovrebbe comunque mantenere invariate le disposizioni della precedente direttiva.

In estrema sintesi, la Cookie Law richiede il consenso informato degli utenti prima di installare cookie sui loro dispositivi e di iniziare il tracciamento.

GDPR

I diritti degli utenti

- **Il diritto ad essere informati:** le organizzazioni devono fornire agli utenti informazioni sulle attività di trattamento dei dati che svolgono. Tali informazioni possono essere fornite per iscritto, anche per via elettronica, tramite una privacy policy. Le informazioni devono essere concise, trasparenti, comprensibili, facilmente accessibili, scritte in un linguaggio chiaro e semplice (soprattutto se rivolte a un minore) e gratuite

- **Il diritto di accesso:** gli utenti hanno il diritto di accedere ai propri dati personali e alle informazioni relative alle modalità di trattamento degli stessi. Su richiesta dell'utente, i titolari del trattamento devono fornire una panoramica delle categorie di dati trattati, una copia degli effettivi dati raccolti ed una descrizione delle modalità del trattamento. È necessario chiarire inoltre le finalità del trattamento, il modo in cui i dati sono stati acquisiti e i soggetti con cui i dati sono stati eventualmente condivisi. Infine, l'organizzazione deve fornire gratuitamente all'utente che ne fa richiesta una copia dei suoi dati personali (qualora l'utente dovesse richiedere più copie, può essere applicato un corrispettivo di ragionevole entità). Il diritto di accesso è strettamente legato al diritto alla portabilità dei dati, sebbene questi due diritti non siano identici. È quindi importante che nell'informativa sulla privacy vi sia una chiara distinzione tra questi due diritti
- **Il diritto di rettifica:** gli utenti hanno il diritto di richiedere la rettifica dei loro dati personali se sono imprecisi o incompleti. Questo diritto implica anche che la rettifica debba essere comunicata a tutti i soggetti terzi coinvolti nel trattamento dei dati in questione, a meno che ciò non sia impossibile o particolarmente difficile. Se richiesto dall'utente, l'organizzazione deve anche informare lo stesso sull'identità di tali soggetti terzi
- **Il diritto di opporsi:** ai sensi del GDPR, gli utenti hanno il diritto di opporsi a determinate attività di trattamento dei loro dati personali effettuate dal titolare del trattamento. In sintesi, l'utente può opporsi al trattamento dei suoi dati ogniqualvolta esso si basi su un interesse legittimo del responsabile del trattamento o sull'esecuzione di un compito di interesse pubblico/esercizio di pubblici poteri o a fini di ricerca e statistica scientifica/storica. L'utente deve motivare la sua opposizione, a meno che il trattamento non sia effettuato a fini di marketing diretto. In quest'ultimo caso, infatti, non è necessaria alcuna motivazione per esercitare tale diritto
- **Il diritto alla portabilità dei dati:** l'utente ha il diritto di ottenere (in un formato elettronico leggibile) i propri dati personali allo scopo di trasferirli ad altro titolare, senza che l'attuale titolare crei alcun ostacolo. Rientrano in questa disposizione sia i dati "forniti" dall'utente, che quelli "osservati"

- **Il diritto alla cancellazione:** quando i dati non sono più utili per le finalità per le quali sono stati raccolti, in caso di revoca del consenso da parte dell'utente o quando i dati personali sono stati trattati in modo illecito, l'utente ha il diritto di chiederne la cancellazione nonché la cessazione di ogni altra forma di diffusione. Il diritto alla cancellazione può essere negato quando i dati personali sono trattati per un interesse pubblico (come la ricerca scientifica), quando i dati sono necessari per la difesa in giudizio o per adempiere a un obbligo di legge, per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui il titolare del trattamento è investito. Il diritto alla cancellazione può essere negato anche quando i dati sono necessari per esercitare il diritto alla libertà di espressione, o quando sono trattati a fini sanitari e di interesse pubblico
- **Il diritto a limitare il trattamento:** l'utente ha il diritto di richiedere la limitazione del trattamento dei suoi dati personali nei casi in cui abbia contestato la loro esattezza, qualora l'utente si sia opposto al trattamento e l'organizzazione stia valutando se vi sia un motivo legittimo che lo escluda, qualora il trattamento sia illecito ma l'utente richieda una limitazione anziché la cancellazione, o qualora i dati non siano più necessari ma l'utente ne abbia bisogno per stabilire, esercitare o difendere una rivendicazione legale. La limitazione deve essere comunicata a tutti i soggetti terzi coinvolti nel trattamento dei dati in questione, a meno che ciò non sia impossibile o particolarmente difficile. Se richiesto dall'utente, l'organizzazione deve anche informare lo stesso sull'identità di tali soggetti terzi
- **Diritti relativi ai processi decisionali automatizzati ed alla profilazione:** gli utenti hanno il diritto di non essere sottoposti a processi decisionali che si basano su un trattamento o una profilazione automatizzati e che producono un effetto legale, o un effetto altrettanto significativo. Le organizzazioni possono adottare decisioni automatizzate solo se necessarie per l'esecuzione di un contratto, autorizzate dalla legislazione del Paese UE applicabile al titolare del trattamento dei dati, prive di effetti giuridici o di analoga rilevanza per l'utente o basate sul consenso esplicito dell'interessato. È possibile prendere decisioni automatizzate senza il consenso esplicito dell'utente solo se riguardano categorie speciali di dati, o per motivi di rilevante interesse pubblico

Trasferimento di dati all'estero

Il GDPR consente il trasferimento dei dati di cittadini UE al di fuori dello Spazio Economico Europeo (SEE) solo se sono soddisfatte determinate condizioni. In particolare, il Paese in cui i dati vengono trasferiti deve avere un livello "adeguato" di protezione dei dati personali, al pari degli standard dell'Unione Europea. In caso contrario, i trasferimenti possono comunque essere consentiti in presenza di clausole contrattuali standard (SCC) o di norme vincolanti d'impresa (BCR)

Il trasferimento dei dati verso gli Stati Uniti è consentito a patto che il responsabile del trattamento aderisca al **Privacy Shield**, o a patto che l'utente abbia espresso il proprio consenso informato (in tal caso, il consenso deve essere fornito sulla base di informazioni sufficientemente precise, comprese quelle relative alla eventuale mancanza di protezione nel Paese terzo).

Il Privacy Shield è un quadro giuridico vincolante che è stato istituito per contribuire a proteggere i diritti degli utenti UE consentendo nel contempo alle società statunitensi di trattare i loro dati senza la necessità di raccogliere uno specifico consenso. Per ulteriori informazioni, consulta l'articolo sul Privacy Shield (in inglese).

Privacy by design e privacy by default

Il tema della protezione dei dati dovrebbe essere preso in considerazione sin dall'inizio della progettazione e dello sviluppo dei processi e delle infrastrutture aziendali. Ciò significa che le regole sulla privacy dovrebbero essere pensate di default al fine di garantire agli utenti un livello di protezione "elevato", e dovrebbero essere messe in atto misure idonee a garantire che il ciclo di vita dei dati trattati sia conforme ai requisiti del GDPR.

La notifica del data breach

Il titolare del trattamento deve informare l'autorità di controllo entro 72 ore dal momento in cui viene a conoscenza di una violazione dei dati personali (data breach). Se il trattamento è effettuato da un responsabile per conto del titolare, il responsabile dovrà darne comunicazione a quest'ultimo immediatamente dopo esserne venuto conoscenza. Anche gli utenti devono essere informati della violazione (entro lo stesso termine) a meno che i dati violati non siano stati protetti mediante cifratura (e quindi resi illeggibili per l'intruso) o, in generale, a meno che sia improbabile che la violazione comporti un rischio elevato per i diritti e le libertà delle persone. In ogni caso, il titolare del trattamento deve tenere un registro delle violazioni verificatesi per poter dimostrare all'autorità di controllo il rispetto di tali disposizioni.

Il Responsabile per la Protezione dei Dati (RPD o DPO)

Il Responsabile per la Protezione dei Dati (RPD), o Data Protection Officer (DPO), è un soggetto con una conoscenza approfondita della legislazione in materia di protezione dei dati, il cui ruolo comprende l'assistenza al titolare del trattamento o al responsabile del trattamento per il

controllo della conformità interna al GDPR, e per la supervisione e l'attuazione della strategia di protezione dei dati. Il DPO dovrebbe inoltre essere competente nella gestione dei processi informatici, nella sicurezza dei dati e in altre questioni critiche relative al trattamento di dati personali e sensibili.

La nomina del DPO è obbligatoria nei seguenti casi:

- quando il trattamento è effettuato da autorità o organismo pubblico;
- quando le attività principali del titolare o del responsabile consistono in trattamenti che richiedono "il monitoraggio regolare e sistematico degli interessati su larga scala";
- quando le attività principali del titolare o del responsabile consistono nel trattamento di dati sensibili o giudiziari.

La nomina di un DPO non si basa pertanto solo sul numero effettivo di dipendenti, ma anche sulla natura dell'attività di trattamento dei dati. Se la tua organizzazione non rientra nelle suindicate categorie, la nomina del DPO non è obbligatoria.

Il Registro del Trattamento

Il GDPR pone in capo ai titolari ed ai responsabili del trattamento **l'obbligo di tenere e mantenere aggiornato** un registro delle particolari attività di trattamento dati effettuate. In genere, questo requisito si applica solo alle organizzazioni con più di 250 dipendenti. Tuttavia, il requisito si applica comunque alle organizzazioni con meno di 250 dipendenti se le loro attività di trattamento:

- non sono occasionali, o;
- includono il trattamento di dati sensibili o di categorie speciali di dati, o;
- possono risultare in un rischio elevato per i diritti e le libertà degli interessati.

Il **Registro del Trattamento deve essere tenuto per iscritto**. È possibile tenere il registro sia in formato cartaceo che elettronico. Tuttavia, il formato elettronico è considerato una best practice in quanto ne agevola l'aggiornamento.

GDPR

Il registro tenuto dal titolare del trattamento deve includere:

il nome e le informazioni di contatto del titolare del trattamento e, se designati, dei responsabili del trattamento e del DPO;
le finalità del trattamento;
una descrizione delle diverse tipologie di utenti e di dati trattati;
le categorie dei soggetti terzi che accedono ai dati, specificando l'eventuale Paese terzo o l'organizzazione internazionale verso cui i dati vengono trasferiti (in caso di trasferimento di dati verso un Paese extra UE);
l'eventuale trasferimento di dati personali verso un Paese extra UE, identificando il Paese terzo o l'organizzazione internazionale verso cui i dati vengono trasferiti, inclusa una documentazione relativa alle misure di sicurezza adottate (se applicabile);
i termini previsti per la cancellazione delle varie categorie di dati (ove possibile);
una descrizione generale delle misure di sicurezza tecniche e organizzative adottate (ove possibile).

Il registro tenuto dal responsabile del trattamento deve includere:

il nome e le informazioni di contatto del titolare del trattamento e degli ulteriori responsabili del trattamento che agiscono per suo conto e, se del caso, del DPO;
le categorie di trattamenti effettuati per conto di ciascun titolare;
l'eventuale trasferimento di dati personali verso un Paese extra UE, identificando il Paese terzo o l'organizzazione internazionale verso cui i dati vengono trasferiti, inclusa una documentazione relativa alle misure di sicurezza adottate (se applicabile);
i termini previsti per la cancellazione delle varie categorie di dati (ove possibile);
una descrizione generale delle misure di sicurezza tecniche e organizzative adottate (ove possibile).

Per quanto riguarda la tenuta dei registri, può essere utile effettuare audit regolari sui dati in possesso dell'organizzazione. Questa pratica è consigliata non solo al fine di soddisfare prontamente gli obblighi di registrazione, ma anche per facilitare la revisione e l'ottimizzazione delle procedure di elaborazione dei dati.

GDPR

IIl Data Protection Impact Assessment (DPIA)

Il Data Protection Impact Assessment (DPIA) è un processo utilizzato per aiutare le organizzazioni a rispettare efficacemente il GDPR e a garantire che i principi di responsabilità, privacy by design e privacy by default siano effettivamente messi in pratica dall'organizzazione. Il processo di DPIA deve essere documentato per iscritto. Sebbene la pubblicazione del DPIA non sia un obbligo formale imposto dal GDPR, è auspicabile che i titolari del trattamento prendano in considerazione l'opportunità di pubblicare in tutto o in parte le loro DPIA come segno di trasparenza e responsabilità, soprattutto nei casi in cui siano coinvolti soggetti pubblici (ad esempio, quando la DPIA è effettuata da un ente pubblico).

Porre in essere degli efficaci processi di DPIA è utile per soddisfare il requisito della "privacy by design" in quanto consente alle organizzazioni di individuare e risolvere i problemi in una fase precoce, riducendo così sia i rischi per la sicurezza dei dati degli utenti, sia il rischio di sanzioni e di danni reputazionali che potrebbero altrimenti verificarsi per l'organizzazione. In generale, la DPIA è obbligatoria solo nei casi in cui l'attività di trattamento dei dati è suscettibile di comportare un rischio elevato per gli utenti (questo vale in particolare per l'introduzione di nuove tecnologie di trattamento). Tuttavia, se non si è sicuri che la propria attività di trattamento rientri o meno in quello che viene considerato un "rischio elevato", si raccomanda di effettuare comunque una DPIA, in quanto si tratta di uno strumento utile a garantire il rispetto della legge.

Le attività di trattamento dei dati considerate ad "alto rischio" includono:

il trattamento di dati sensibili;
il monitoraggio sistematico di un'area accessibile al pubblico (ad esempio, tramite video sorveglianza);
le situazioni in cui vengono effettuate valutazioni automatizzate e approfondite dei dati personali al fine di influenzare in modo significativo decisioni rilevanti per la vita dell'utente.

Le valutazioni d'impatto (DPIA) possono essere richieste anche in altre circostanze (sulla base di una valutazione caso per caso), tra cui il trattamento dei dati relativi a persone vulnerabili (come bambini o anziani), il trasferimento di dati al di fuori del territorio UE e il trattamento di dati utilizzati per la profilazione. Ulteriori informazioni sui casi in cui è necessario effettuare una DPIA sono disponibili qui.

La relazione prodotta a seguito di un processo di DPIA dovrebbe includere:

una descrizione completa dei dati trattati;
lo scopo dell'attività di trattamento (e, se del caso, le informazioni sugli interessi legittimi del responsabile del trattamento);
una valutazione dell'ambito e della necessità dell'attività di trattamento in relazione alla finalità perseguita;
una valutazione del rischio per gli utenti;
le misure in atto per far fronte a tale rischio.

Le conseguenze del mancato adeguamento

Le conseguenze legali per il mancato rispetto del GDPR possono consistere in sanzioni pecuniarie fino a 20 milioni di euro o fino al 4% del fatturato mondiale annuo dell'organizzazione (a seconda di quale sia il maggiore tra questi due valori). Altrettanto rilevanti sono anche gli altri provvedimenti che possono essere attuati nei confronti delle organizzazioni che hanno commesso una violazione. Tali provvedimenti comprendono richiami ufficiali (per violazioni avvenute per la prima volta), verifiche periodiche sulla protezione dei dati e danni da responsabilità.

Il GDPR conferisce agli utenti il diritto esplicito di presentare un reclamo presso un'autorità di controllo qualora ritengano che il trattamento dei loro dati personali sia stato effettuato in violazione delle disposizioni del regolamento. Ad esempio, se viene presentata una segnalazione all'autorità in merito a un'istanza di violazione della normativa, l'autorità può scegliere di effettuare una verifica dei processi di trattamento dei dati da parte dell'organizzazione. Qualora si accerti che alcune attività di trattamento siano state svolte in modo illecito, non solo viene comminata una sanzione pecuniaria, ma all'organizzazione può anche essere vietato di fare un ulteriore uso sia dei dati oggetto del reclamo che dei dati acquisiti utilizzando meccanismi analoghi. Ciò significa che se l'uso improprio riguardava, ad esempio, la raccolta di un indirizzo email, l'organizzazione rischia di non poter utilizzare l'intero database di email in suo possesso.

Il GDPR conferisce inoltre agli utenti il diritto al risarcimento di eventuali danni derivanti dall'inosservanza delle norme da parte di un'organizzazione, rendendo in tal modo i trasgressori suscettibili di essere citati in giudizio.