PUBLIC

ROQUETTE
Offering the best of nature™

Privacy & Data Protection

IN CHE MODO CI IMPEGNIAMO A TUTELARE LA PRIVACY E PROTEGGERE I DATI QUOTIDIANAMENTE

Legal & Compliance

Le principali sfide di Roquette in materia di conformità

Sotto la guida della Direzione generale, la conformità e la sua gestione all'interno di Roquette sono di competenza dell'Ufficio "Legal & Compliance" del Gruppo che ha creato un Ufficio Compliance.

L'Ufficio Compliance si occupa del Codice di condotta di Roquette, del suo aggiornamento e della sua attuazione.

Si occupa anche delle tre aree principali seguenti:

- Sicurezza finanziaria,
- Etica professionale e
- Tutela della privacy e protezione dei dati.

È stato quindi messo a punto un Programma di conformità in continua evoluzione per garantire l'irreprensibilità giuridica e finanziaria della nostra attività.

Qual è il ruolo del Programma di conformità?

Il suo ruolo è quello di instillare **valori etici** e di adottare misure conformi a **requisiti legali, standard** e **buone pratiche.**

Il nostro programma facilita l'implementazione di procedure che garantiscono la conformità con le regole applicabili a Roquette.

I nostri quattro valori – **autenticità, eccellenza, lungimiranza, benessere** – costituiscono la base solida sulla quale agiamo **ogni giorno**.

Tenete a mente che oggigiorno, un'azienda sostenibile è un'azienda etica.
E la società del futuro è la società trasparente.

Pensare globalmente
Agire localmente

Editoriale

I principi della Tutela della privacy e della protezione dei dati fanno parte degli standard definiti nel Codice di condotta.

Tutti i dipendenti e tutti i soggetti terzi che entrano in contatto con Roquette hanno diritto alla privacy. Per questo motivo, Roquette dedica la massima cura alla protezione e alla corretta gestione dei dati personali.

I dati personali sono informazioni che consentono, direttamente o indirettamente, di identificare una persona fisica (nome, data di nascita, codice fiscale, foto, indirizzo e-mail, ID del computer, ecc.).

La protezione dei dati personali è un diritto fondamentale che garantisce la privacy

La protezione di questi dati garantisce a ogni individuo il diritto di controllare la raccolta, il trattamento, l'utilizzo e la distribuzione dei dati che lo riguardano.

I dati personali devono essere utilizzati in modo corretto per scopi specifici, espliciti e legittimi e devono essere conservati solo per il periodo di tempo necessario alle finalità del trattamento in questione.

In Europa, il trattamento dei dati personali è stato regolato dal Regolamento generale sulla protezione dei dati (GDPR) che è entrato in vigore il 25 maggio 2018.

Poiché la legislazione sulla tutela della privacy e la protezione dei dati personali varia da paese a paese, e poiché Roquette è presente a livello internazionale, il Gruppo ha adottato una Politica di Gruppo relativa alla protezione dei dati personali. Questa Politica si applica a tutti i dipendenti del Gruppo a livello globale.

Questa Guida spiega la condotta corretta da adottare nelle attività quotidiane per conformarsi ai principi di protezione dei dati personali e ai requisiti della nostra Politica.

Jennifer GODIN, Responsabile Protezione dei Dati - Data Protection Officer

Déléguée à la protection des données

Indice

Finalità

Cos'è la Politica per la tutela della privacy e la protezione dei dati?

Il Gruppo Roquette ha definito una Politica per la tutela della privacy e la protezione dei dati (la "Politica") al fine di affrontare nel modo migliore possibile le questioni relative alla tutela della privacy e alla protezione dei dati in linea con la sua immagine, i suoi interessi e la legislazione applicabile in materia di protezione dei dati.

Questa Politica definisce i principi e i requisiti per la protezione delle informazioni personali e indica le regole che tutti i dipendenti, i manager, i direttori e le terze parti sono tenuti a rispettare in termini di tutela della privacy e protezione dei dati quando agiscono per conto di Roquette.

I principi e le regole di questa Politica di protezione dei dati personali sono specificati in una piattaforma documentaria con tre livelli:

- Impegno della dirigenza: Codice di Condotta.
- Regole interne: Manuale di protezione dei dati personali e direttive in Q-Docs.
- Documentazione sul sistema di gestione della protezione dei dati (DPMS): Procedure, linee guida, metodologie, formazione, ecc.

Tutta la documentazione è conforme con i requisiti giuridici e regolamentari relativi alla protezione dei dati.

Cos'è la Guida di Buona Condotta per la Tutela della Privacy e la Protezione dei Dati?

La Guida per la tutela della privacy e la protezione dei dati (la "Guida") può aiutarci a attuare e conformarci alla Politica per la tutela della privacy e la protezione dei dati.

Presenta, in maniera semplificata, regole e buone pratiche conformi alle direttive del Gruppo e i requisiti legislativi e normativi applicabili alla nostra società in termini di protezione dei dati.

È suddivisa in tematiche ispirate al Codice di condotta, tra le quali "Tutela della privacy e protezione dei dati" è uno degli argomenti correlati alla conformità.

Descrizione

A chi si applica la Guida di Buona Condotta per la Tutela della Privacy e la Protezione dei Dati?

La Politica e la Guida rappresentano una base comune per tutte le filiali in tutto il mondo. Si applicano a:

- Tutti i dipendenti, direttori e manager ("i Dipendenti")
- Tutti i terzi che agiscono per conto di Roquette, come:
  - Appaltatori, inclusi consulenti, liberi professionisti e personale temporaneo
  - Formatori
  - Staff di un'entità non appartenente a Roquette
  - Lavoratori interinali
  - Altri rappresentanti
  - E qualsiasi altra terza parte impiegata o retribuita da Roquette.

Dove trovare la Guida di Buona Condotta per la Tutela della Privacy e la Protezione dei Dati?

Tutti i dipendenti e i terzi che agiscono per conto di Roquette devono conoscere e rispettare i principi in materia di privacy e protezione dei dati contenuti nella nostra documentazione e in particolare nella presente Guida.

La Guida è a portata di clic sul Portale ONE:

Funzioni Globali > Protezione dei Dati > Guida di Buona Condotta.

Questa Guida è oggetto di una comunicazione dedicata, accompagnata da un kit strumenti con corsi di e-learning sui principi di tutela della privacy e protezione dei dati (definiti dagli standard internazionali e dai requisiti specifici dell'GDPR).

Questo corso di formazione fa parte del programma di inserimento sulla protezione dei dati.

Responsabilità

Chi è responsabile dell'attuazione dei principi operativi?

La riservatezza dei dati, e la responsabilità che ne deriva, sono di importanza cruciale per tutti all'interno della nostra organizzazione.

Tutti noi abbiamo la responsabilità di rispettare i principi operativi descritti nella documentazione DPMS fornita dal team dell'ufficio Compliance e dalla rete di protezione dei dati. La presente Guida supporta questa implementazione e accresce il nostro livello di conformità.

Come possiamo essere certi di prendere la decisione giusta?

La Guida è stata pensata per aiutarci a gestire tutte quelle situazioni della vita lavorativa che possono sollevare questioni relative alla privacy. Non può tuttavia prevedere ogni singola situazione che potremmo doverci trovare ad affrontare durante lo svolgimento della nostra attività professionale.
In caso di dubbi relativi alla condotta da adottare, dobbiamo fare appello al buon senso e porci, in qualsiasi momento, le seguenti domande:

- Il comportamento in questione è conforme alla legge?
- Ha ripercussioni positive su di me e sull'azienda?
- Ne parlerei con un amico, un familiare o un collega?
- Mi sentirei a mio agio se fosse reso pubblico?

Se la risposta a tutte queste domande è 'No', non dobbiamo procedere. In caso di dubbi, dobbiamo rivolgerci al Responsabile Protezione dei Dati (Data Protection Officer) del Gruppo o a altri contatti pertinenti (vedere informazioni di contatto nella sezione "Domande o dubbi").

Cosa accade se non ci conformiamo ai principi di tutela della privacy e protezione dei dati?

Il mancato rispetto dei Principi può ripercuotersi negativamente sull'azienda. Le conseguenze possono essere molto gravi, sia per l'azienda sia per le persone coinvolte (sanzioni disciplinari, multe, reclusione, danno d'immagine, ecc.).

Tutte le segnalazioni di violazioni dei Principi effettive o sospette saranno prese in seria considerazione. Procederemo a un'indagine rapida, equa e conforme ai requisiti legislativi.

In relazione alla natura della Violazione dei dati in essere, possono essere adottate misure disciplinari ai sensi della legislazione locale e dei regolamenti aziendali vigenti.

A tutti i dipendenti è richiesta la piena collaborazione in caso di indagine. Roquette proteggerà la riservatezza delle persone coinvolte.

Domande o dubbi

Dipendenti, terzi che agiscono per conto di Roquette e altri interessati sono incoraggiati a porre domande o sollevare dubbi allo scopo di aiutare Roquette a prevenire e ridurre eventuali danni alla società.

Che tipo di situazione può essere segnalata?

Possono essere segnalate domande, violazioni potenziali o effettive ai Principi di tutela della privacy e protezione dei dati, ai regolamenti aziendali o alla legislazione applicabile.

Chi dobbiamo contattare?

In caso di Violazione dei dati contattare il Responsabile della protezione dei dati a dpo@Roquette.com e/o segnalare un incidente tramite il nostro modulo web di "Privacy Alert".

Se avete bisogno di segnalare una potenziale violazione della conformità, potete contattare il vostro punto di contatto abituale o segnalare un problema tramite il dispositivo Speakup©. Tutte le segnalazioni ricevute tramite questo dispositivo vengono trattate in modo riservato, nel rispetto delle leggi e delle normative vigenti.

SpeakUp®

Roquette non tollererà alcuna forma di rappresaglia o ritorsione contro un collaboratore o terzi che abbiano riferito in buona fede una supposta o effettiva violazione dei Principi di tutela della privacy e protezione dei dati o della legislazione applicabile.

Pertanto, qualora l'autore di una segnalazione professionale dovesse identificarsi, la sua identità deve essere trattata in modo riservato dall'organizzazione al fine di evitare il rischio di rappresaglie, discriminazioni o misure disciplinari contro di lui/lei per aver denunciato i fatti.

Rispetto delle leggi e dei regolamenti

Tutti, in qualsiasi filiale del Gruppo, devono rispettare le leggi e i regolamenti vigenti in materia di Protezione dei dati.

Laddove la legislazione locale sia più restrittiva rispetto alla nostra Politica e alla Guida, prevarrà su questi ultimi.

Altrimenti (assenza di legislazione locale o legislazione meno restrittiva), saranno le buone pratiche interne a prevalere, nei limiti consentiti dalla legge.

Ricordiamo che:

- Tutte le normative locali e applicabili devono essere attuate il prima possibile.
- Tutti noi dobbiamo essere consapevoli che qualsiasi violazione delle leggi e dei regolamenti può comportare sanzioni civili e/o penali a carico della persona coinvolta e dell'azienda.
- La protezione delle persone fisiche in termini di trattamento dei dati personali è un diritto fondamentale.
- I principi e le regole sulla protezione delle persone fisiche relativamente al trattamento dei loro dati personali devono, indipendentemente dalla nazionalità o dal luogo di residenza, rispettare i loro diritti e le loro libertà fondamentali, nello specifico il diritto alla protezione dei dati personali.
- Il diritto alla protezione di dati personali non è un diritto assoluto; va considerato in relazione alla funzione nella società e messo in relazione con altri diritti fondamentali, conformemente al principio di proporzionalità.

Quale Paese ha adottato una legislazione specifica di protezione dei dati o ha un'autorità garante della protezione dei dati?

Per una panoramica, consultare questa mappa: https://www.cnil.fr/en/data-protection-around-the-world.

Le nostre responsabilità:

- In qualsiasi circostanza, dobbiamo rispettare le leggi e i regolamenti in materia di protezione dei dati applicabili nei paesi degli interessati e tutte le norme in vigore in ciascuna sede dell'azienda.

- Come parte dell'attività professionale, dobbiamo riferire qualsiasi comportamento che riteniamo contrario alle leggi e ai regolamenti sulla protezione dei dati (es.: GDPR) al Responsabile della protezione di dati (Data Protection Officer) all'indirizzo dpo@Roquette.com e il dispositivo di allarme confidenziale Roquette: Speakup©.

- Dobbiamo adottare misure per la protezione dei dati personali che siano appropriate e proporzionate al contesto, agevolando nello stesso tempo la conformità con altre leggi e regolamenti. Analogamente, le azioni per conformarsi alle leggi e ai regolamenti applicabili al Gruppo devono rispettare le regole e le buone pratiche per la protezione dei dati personali (ad esempio: nel programma di conformità anti-subornazione e corruzione, dobbiamo assicurare la protezione di chi effettua una segnalazione attraverso misure di riservatezza e protezione dei suoi dati personali).

Voi siete soggetti al Regolamento Generale sulla Protezione dei Dati (GDPR)?

Rientrate nella sfera di applicazione dell'GDPR in qualità di **responsabile** (1) o **titolare del trattamento** (2):

- se siete stabiliti nell'Unione oppure;
- se non siete stabiliti nell'Unione quando: le "attività di trattamento riguardano
  - l'offerta di merci o la prestazione di servizi ai suddetti interessati nell'Unione;
  - oppure il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione".

Testo ufficiale: Articolo 3 dell'GDPR sull'Ambito di applicazione territoriale

(1) e (2): Vedere definizioni a pagina 38.

Principi di protezione dei dati

I dati personali devono essere:

- protetti.
- accurati e aggiornati.
- trattati in modo equo e lecito.
- trattati per finalità determinate.
- adeguati, pertinenti e non eccedenti.
- conservati per un periodo di tempo limitato e determinato.
- trattati conformemente ai diritti dell'interessato.
- protetti da misure legislative adeguate in caso di trasferimento in altri paesi.

I diritti dell'interessato:

Ai sensi della legislazione e dei regolamenti applicabili, l'interessato ha il diritto di accesso ai dati personali e di rettifica degli stessi, di opporsi al loro trattamento per ragioni legittime oltre al diritto di cancellazione degli stessi per ragioni legittime, il diritto alla portabilità dei dati e il diritto alla limitazione del trattamento dei dati personali che lo riguardano.

Per esercitare questi diritti compilare il modulo disponibile su: Roquette.com/Protezione dei dati.

Per qualsiasi richiesta, contattare il Responsabile della protezione dei dati (Data Protection Officer) (dpo@Roquette.com).

Le nostre responsabilità:

Dobbiamo:

- Rispettare la legislazione locale e le norme della Politica del Gruppo in materia di protezione di dati personali.
- Notificare al Responsabile della protezione dei dati (Data Protection Officer) qualsiasi nuovo trattamento o eventuali modifiche.
- Non raccogliere, usare, rivelare né archiviare dati di natura personale tranne che per finalità specifiche, legittime e necessarie.
- Accertarci che gli interessati siano stati informati che stiamo raccogliendo i loro dati.
- Proteggere tali dati nelle fasi di raccolta, trattamento, uso, comunicazione, archiviazione o trasferimento.
- Garantire la sicurezza e la confidenzialità dei dati trattati.
- Conservare i dati solo per il tempo necessario per il trattamento nel rispetto delle leggi applicabili.
- Contattare il Responsabile della protezione dei dati (Data Protection Officer) nel caso in cui si verifichi un incidente di sicurezza che coinvolge i dati personali.

Formiamo i nostri dipendenti e miglioriamo i nostri processi interni.

Home

Rischio per la privacy

Cos'è un rischio per la privacy?

Un rischio è uno scenario ipotetico che descrive un evento temuto e tutte le minacce che ne consentirebbero il verificarsi. Più nello specifico, descrive:

- in che modo le fonti di rischio (ad es.: un dipendente corrotto da un concorrente)
- potrebbero sfruttare la vulnerabilità delle risorse di supporto (ad es.: il sistema di file management che consente la manipolazione dei dati)
- in un contesto di minacce (ad es.: uso indebito attraverso l'invio di e-mail)
- e permettere che si verifichi l'evento temuto (ad es.: accesso illegittimo ai dati personali)
- sui dati personali (ad es.: file di un cliente)
- influendo in questo modo sulla privacy degli interessati (ad es.: sollecitazioni non gradite, sensazione di invasione della privacy, problemi di natura personale o professionale).

Effetto dell'incertezza sulla privacy

La gravità rappresenta l'entità di un rischio. Viene in primo luogo stimata in termini di ampiezza degli impatti potenziali (**fisico, materiale, morale**) sugli interessati tenendo conto di controlli esistenti, programmati o aggiuntivi.

Esempio:

Il rischio più importante presentato dal sistema di segnalazione professionale per chi effettua una segnalazione: rischio di rappresaglie, discriminazioni o misure disciplinari adottate contro di lui/lei per aver denunciato i fatti.

Ricordiamo che:

I diritti individuali si applicano indipendentemente dal livello di rischio del trattamento.

Tuttavia, ci sarà chiesto di modulare la conformità della protezione dei dati in base al livello di rischio posto dalle attività di trattamento dei dati personali in relazione ai diritti fondamentali e alle libertà degli individui.

Il GDPR dà ulteriore impulso a questa pratica. Conseguentemente, le operazioni di trattamento che implicano bassi rischi per i diritti e le libertà fondamentali degli individui, generalmente possono comportare un numero inferiore di obblighi in termini di conformità, mentre le operazioni di trattamento a "alto rischio" comporteranno ulteriori obblighi in termini di conformità, quali la Valutazione dell'impatto della protezione dei dati (DPIA) (1)

Le nostre responsabilità:

La valutazione del rischio riveste un'importanza cruciale. Ai sensi dell'GDPR, la considerazione del rischio sottende la responsabilità organizzativa e il trattamento di tutti i dati.

Dobbiamo effettuare delle valutazioni del rischio come parte delle DPIA per il trattamento che presenta rischi elevati, come pure in riferimento a molti altri requisiti dell'GDPR, inclusi la sicurezza dei dati, le notifiche in materia di sicurezza e violazione dei dati, Privacy by Design, interesse legittimo, limitazione delle finalità e trattamento equo.

(1): Vedere definizione a pagina 58.

Rischi in caso di non conformità

Le persone giuridiche e fisiche che non rispettano la legge e il regolamento sulla protezione dei dati (ad es. GDPR) rischiano sanzioni e ammende pecuniarie sotto forma di:

Sanzioni penali:

- Reclusione.
- Multe per soggetti giuridici.

Sanzioni civili:

- Risarcimento danni.

Sanzioni amministrative:

- Notifica formale.
- Diffida.
- Ingiunzione.
- Limitazione temporanea o definitiva del trattamento.
- Revoca di una certificazione o ingiunzione di revoca di una certificazione.
- Sospensione del trasferimento di dati.
- Ingiunzione a cessare il trattamento o revoca dell'autorizzazione.
- Pubblicazione delle sanzioni imposte.
- Sanzioni senza previa notifica formale (criterio d'urgenza).
- A seconda della violazione, un'ammenda amministrativa.

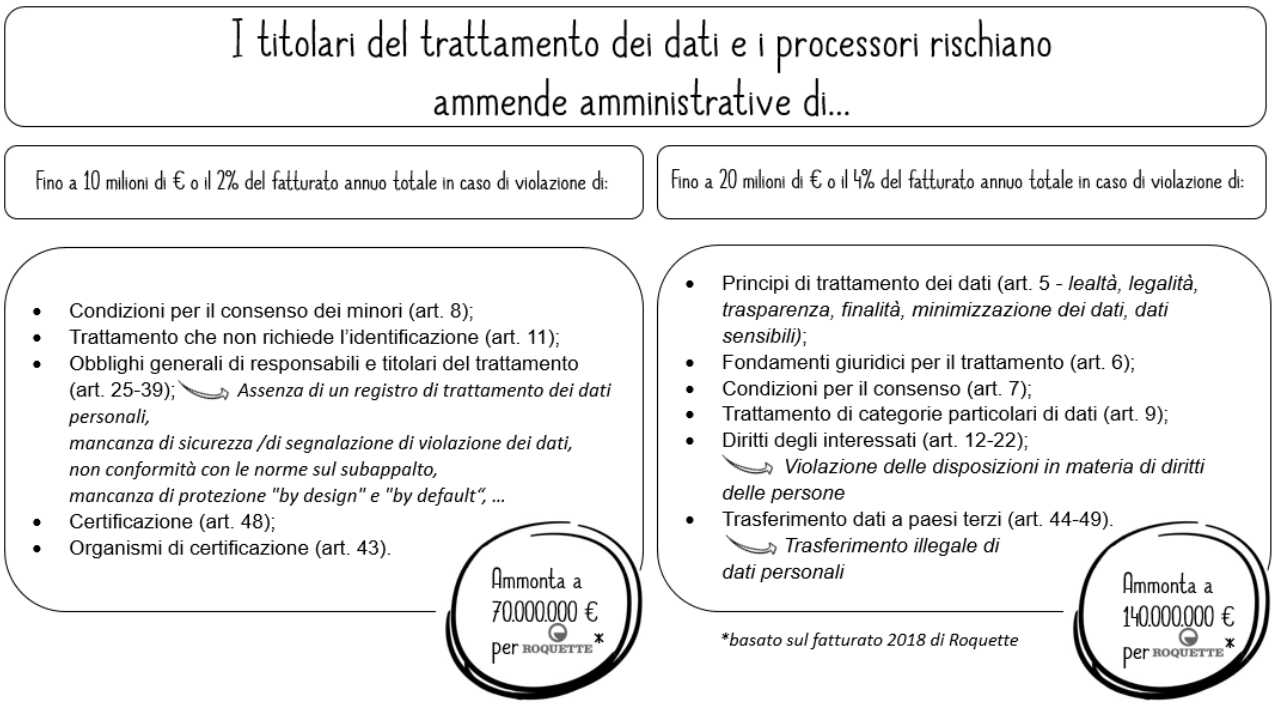
Costi significativi:

- Mancato guadagno dovuto al danno in termini di immagine.

A quanto ammonta l'ammenda amministrativa più elevata ai sensi dell'GDPR?

Le ammende sono discrezionali piuttosto che obbligatorie. Devono essere applicate caso per caso e devono essere "efficaci, proporzionate e dissuasive".

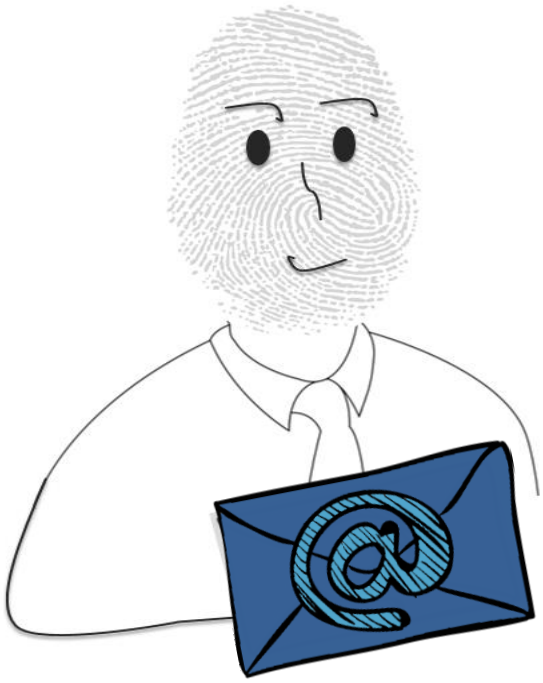
Le ammende sono applicate in base agli articoli specifici del Regolamento che sono stati violati dall'organizzazione.



In cosa possono consistere le sanzioni penali?

Alcuni esempi in base alla legislazione francese:

- L'atto di raccogliere dati personali con mezzi fraudolenti, iniqui o illegittimi può essere punibile con cinque anni di reclusione e una multa fino a 300.000 € (Codice penale Art. 226-18).
- Al fine di garantire un reale diritto di protezione a chi denuncia una violazione, la legge anticorruzione (Sapin II) punisce severamente qualsiasi ostacolo a una segnalazione. La riservatezza della segnalazione è un elemento essenziale del regolamento. Pertanto, la divulgazione di elementi riservati della segnalazione (identità della persona che l'ha effettuata, dell'imputato, informazioni fornite a supporto della segnalazione), fatta eccezione per l'autorità giudiziaria, è punibile con due anni di reclusione e una multa di 30.000 €.



1 I nostri standard nelle RELAZIONI CON GLI INTERESSATI

Cultura della privacy

La **protezione dei dati** è una serie di leggi, regolamenti e buone pratiche che regolano la raccolta e l'uso di dati personali.

Per **Dati personali** si intende qualsiasi informazione relativa a una persona fisica identificata o identificabile.

La **Riservatezza dei dati** si riferisce al trattamento dei dati personali.

Chi è interessato?

La riservatezza dei dati, e la responsabilità che ne deriva, sono di importanza cruciale per tutti all'interno della nostra organizzazione.

Perché è importante?

Il trattamento errato dei dati personali può avere ripercussioni serie sull'organizzazione, sui dipendenti e sui clienti.

La violazione della privacy può comportare sanzioni finanziarie molto pesanti, avversione della stampa, rovina della reputazione, perdita di attività commerciali e, per quel che riguarda i dipendenti, richieste di risarcimento e probabilmente denunce in caso di violazione della loro privacy, nonché la prospettiva di azioni disciplinari in altri casi. Abbiamo tutto l'interesse a trattare i dati nel modo corretto.

Ricordiamo che:

- Tutti i dipendenti di Roquette devono essere consapevoli del ruolo e delle responsabilità che ricoprono in termini di protezione dei dati personali. La sensibilizzazione ha lo scopo di rafforzare la cultura di rispetto della privacy e di protezione dei dati personali all'interno di Roquette.

[DDPG001EN – Regola 1]

- Deve essere organizzata la formazione dei dipendenti sull'attuazione della Politica di protezione dei dati personali.

[DDPG001EN – Regola 2]

PENSATE ALLA PRIVACY

È una nostra responsabilità!

Per funzionare al meglio, la nostra azienda deve utilizzare i dati personali di clienti e dipendenti.
Sono stati affidati a noi e dobbiamo trattarli adeguatamente.

Ogni singolo dipendente è responsabile del rispetto delle disposizioni legislative in materia di protezione dei dati.

È in gioco la nostra reputazione!

Una buona reputazione è difficile da conquistare e facile da perdere.

Gestire con cura le informazioni di clienti e dipendenti è fondamentale per proteggere la nostra reputazione.

Siete VOI la nostra migliore difesa contro il rischio di danni alla reputazione.

È una questione di rispetto!

Per meritare la fiducia che clienti e dipendenti ripongono in noi, dobbiamo rispettare le loro scelte in materia di utilizzo dei dati.

È tutto nelle tue mani!

Siamo tutti chiamati a garantire che i dati personali di clienti e dipendenti vengano conservati al sicuro e trattati in modo confidenziale.
Occorre prestare particolare attenzione a tutte le informazioni che devono essere spedite o fatte uscire dall'azienda.

Formiamo i nostri dipendenti e miglioriamo i nostri processi interni.

- Codice di condotta – Tutela della privacy e protezione dei dati - pag. 42 – 43.
- Per i neoassunti: Alcune informazioni e l'e-Learning sono forniti durante il programma di inserimento globale.
- Per i dipendenti: La formazione è caricata su piattaforma di apprendimento.
- Per i coordinatori della protezione dei dati: La documentazione è condivisa sulla Community "Rete protezione dati".
- Per tutti: Ulteriori informazioni sono disponibili sul portale interno > Protezione dei dati.

Trattamento dei dati personali

Trattamento dei dati personali indica qualsiasi operazione o serie di operazioni eseguite sui dati personali o su una serie di dati personali, tramite mezzi automatizzati o no, quali la raccolta, la registrazione, l'organizzazione, la strutturazione, l'archiviazione, l'adattamento o l'alterazione, il recupero, la consultazione, l'utilizzo, la divulgazione tramite trasmissione, la diffusione o la messa a disposizione, l'allineamento o combinazione, restrizione, cancellazione o distruzione.

Un requisito della Protezione dei dati (e dell'GDPR) del quale dovrete essere a conoscenza è la necessità dell'esistenza di un "fondamento giuridico" per la raccolta dei dati personali. I fondamenti giuridici possono variare in base alla legislazione locale.

Qual è il "fondamento giuridico" per il trattamento dei dati personali?

Dovete essere in grado di rispondere chiaramente alla domanda:

"Come avete ottenuto il [singolo dato] e perché siete autorizzati ad averlo?"

Più nello specifico, significa che dovete rispettare almeno uno dei sei fondamenti giuridici relativi al trattamento dei dati. Ai sensi dell'GDPR, non è possibile trattare i dati senza:

1. Consenso
2. Contratto
3. Obbligo legale
4. Interessi vitali
5. Servizio pubblico
6. Interesse legittimo

Legittimità, equità e trasparenza

Le nostre responsabilità:

Dobbiamo applicare delle regole per garantire il trattamento legittimo dei dati personali.

Regole	Riferimento Q-Docs	Riferimento GDPR
• Agire nel rispetto dei principi di liceità, equità e trasparenza quando si raccolgono i dati	DDPG002EN Regola 1	Art. 5 1. a)
• Dimostrare che viene rispettato il consenso dell'interessato (quando richiesto)	DDPG002EN Regola 2	Art. 7
• Rispettare le finalità determinate durante la raccolta dei dati	DDPG002EN Regola 3	Art. 5 1. b)
• Limitare le informazioni raccolte in forma cartacea o digitale al minimo strettamente necessario	DDPG002EN Regola 4	Art. 5 1. c)
• Limitare l'archiviazione dei dati al minimo strettamente necessario	DDPG002EN Regola 5	Art. 5 1. e)
• Adottare le misure per il trasferimento dei dati personali a paesi terzi o organizzazioni internazionali	DDPG002EN Regola 6	Art. da 44 a 50

Formiamo i nostri dipendenti e miglioriamo i nostri processi interni.

Diritti degli interessati

Interessato indica una persona fisica che può essere identificata, direttamente o indirettamente, nello specifico attraverso un identificativo quale un nome, un numero di identificazione, dati di localizzazione, un identificativo online o uno o più fattori caratteristici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di quella persona fisica.

Cosa si intende per "interessato"?

Si tratta di un termine tecnico che indica la persona alla quale si riferiscono i dati personali in questione.

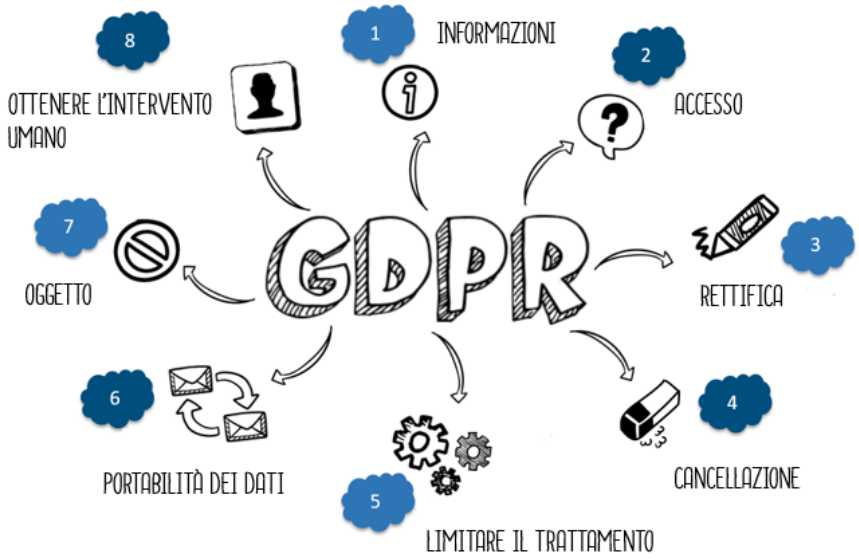
Che cos'è una richiesta di accesso?

Uno dei diritti principali che le leggi sulla protezione dei dati vigenti assegnano alle persone è il diritto di accesso ai loro dati personali.

Una persona può inviarvi una "richiesta di accesso" chiedendo di comunicargli/le le informazioni personali che possedete su di lui/lei e di fornirgli/le una copia di queste informazioni. Nella maggior parte dei casi siete tenuti a rispondere a una richiesta di accesso valida entro 30 (*) giorni di calendario dalla data di ricevimento.

(*): Tale periodo può variare a seconda della legislazione applicabile o della natura dell'attività di trattamento dei dati.

Quali sono gli altri diritti degli interessati?



Le nostre responsabilità:

Dobbiamo applicare delle regole per garantire i diritti degli interessati.

Regole	Riferimento Q-Docs	Riferimento GDPR
• Accertarsi che le note legali siano conformi agli obblighi	DDPG006EN Regola 1	Art. 12
• Consentire alle persone interessate di esercitare i diritti di accesso	DDPG006EN Regola 2	Art. 15
• Consentire alle persone interessate di esercitare il diritto di rettifica	DDPG006EN Regola 3	Art. 16
• Consentire alle persone interessate di esercitare il diritto di portabilità dei dati	DDPG006EN Regola 4	Art. 20
• Consentire alle persone interessate di esercitare il diritto di cancellazione (“diritto all’oblio”)	DDPG006EN Regola 5	Art. 17
• Consentire alle persone interessate di esercitare il diritto di limitazione di trattamento	DDPG006EN Regola 6	Art. 18
• Notificare la rettifica o la cancellazione dei dati personali o la limitazione del trattamento	DDPG006EN Regola 7	Art. 19
• Controllare il processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione	DDPG006EN Regola 8	Art. 22

Per saperne di più...

Informativa sulla privacy

Il diritto a essere informati dell'uso dei propri dati personali

Dobbiamo informare voi in quanto dipendenti e tutte le terze parti che hanno una relazione con Roquette se stiamo usando i vostri/loro dati personali.

Dobbiamo fornire informazioni dettagliate sui seguenti punti:

- Perché Roquette sta usando i dati.
- Quale tipo di dati sta usando Roquette.
- Come saranno raccolti i dati.
- I vostri/loro diritti.
- Da dove provengono i dati.
- Informare dell'intenzione di Roquette di trasferire i dati a terzi, inclusi i vostri/loro nomi e i motivi del trasferimento.
- Informare del trasferimento dei dati in un'altra giurisdizione, incluso il paese in questione e di cosa verrà fatto dei dati.
- Se Roquette usa i dati nella profilazione (un tipo di trattamento automatizzato nel quale i dati personali sono utilizzati per analizzare o predire cose quali le prestazioni lavorative, la situazione economica, la salute).
- Come contattare il DPO.
- Se pertinente, il diritto a inoltrare un reclamo all'autorità di vigilanza.

Tutto ciò viene definito **Informazioni sulla privacy** o **Informativa sulla privacy**.

Le informazioni vanno fornite nel momento in cui Roquette raccoglie i dati. Se Roquette ottiene i dati da un'altra fonte, deve fornire informazioni sulla privacy. Può essere fatto sotto forma di informativa sulla privacy.

Questo è ciò che viene definito **il diritto a essere informato**.

Regole	Riferimento Q-Docs	Riferimento GDPR
• Accertarsi che le note legali siano conformi agli obblighi	DDPG006EN Regola 1	Art. 12

Esempi:

- Informativa sulla privacy sul sito web di Roquette disponibile all'indirizzo: https://www.Roquette.com/data-protection.
- Informativa sulla privacy sui processi HR su Workday@Roquette disponibile su ONE: Spazio dipendenti>Workday@Roquette.

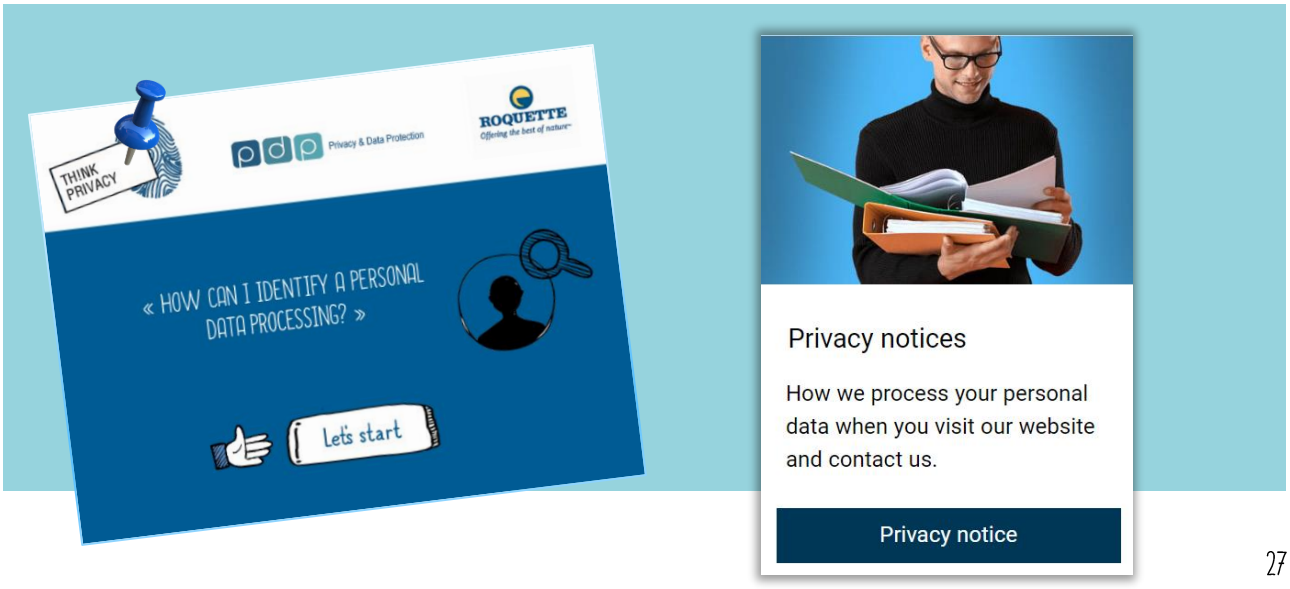
Quando Roquette può esimersi dall'informare voi/loro delle sue attività?

Generalmente siamo tenuti a fornire le informazioni sulla privacy, ma in alcuni casi non abbiamo tale obbligo. Questi casi includono l'eventualità in cui:

- già si dispone dell'informativa sulla privacy e nulla è cambiato,
- fornire informazioni sulla privacy è impossibile o richiederebbe uno "sforzo sproporzionato", oppure
- fornire informazioni sulla privacy renderebbe impossibile l'utilizzo dei dati o danneggerebbe seriamente i motivi per cui vengono utilizzati.

Nota: Quando sono necessarie misure provvisorie per evitare l'occultamento o la distruzione di prove, tale informazione può essere rilasciata dopo l'adozione delle misure provvisorie.

Formiamo i nostri dipendenti e miglioriamo i nostri processi interni.



Minimizzazione dei dati

Cosa comporta il principio di minimizzazione dei dati?

GDPR - Articolo 5(1)(c) afferma:

> "1. I dati personali saranno:
>
> (c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati)"

I documenti in forma cartacea o digitale messi a punto dalle funzioni Global per la raccolta dei dati devono contenere solo i campi di dati strettamente necessari per la finalità del trattamento al fine di evitare di raccogliere dati non giustificati dal trattamento.

Le nostre responsabilità:

Dobbiamo accertarci che i dati personali che stiamo trattando sono:

- adeguati – sufficienti a raggiungere in modo appropriato la finalità indicata;
- pertinenti – siano ragionevolmente collegati a quella finalità; e
- limitati a quanto necessario – non è possibile conservare più di quanto necessario per quella finalità.

Regole	Riferimento Q-Docs	Riferimento GDPR
• Limitare le informazioni raccolte in forma cartacea o digitale al minimo strettamente necessario	DDPG002EN Regola 4	Art. 5 1. c)

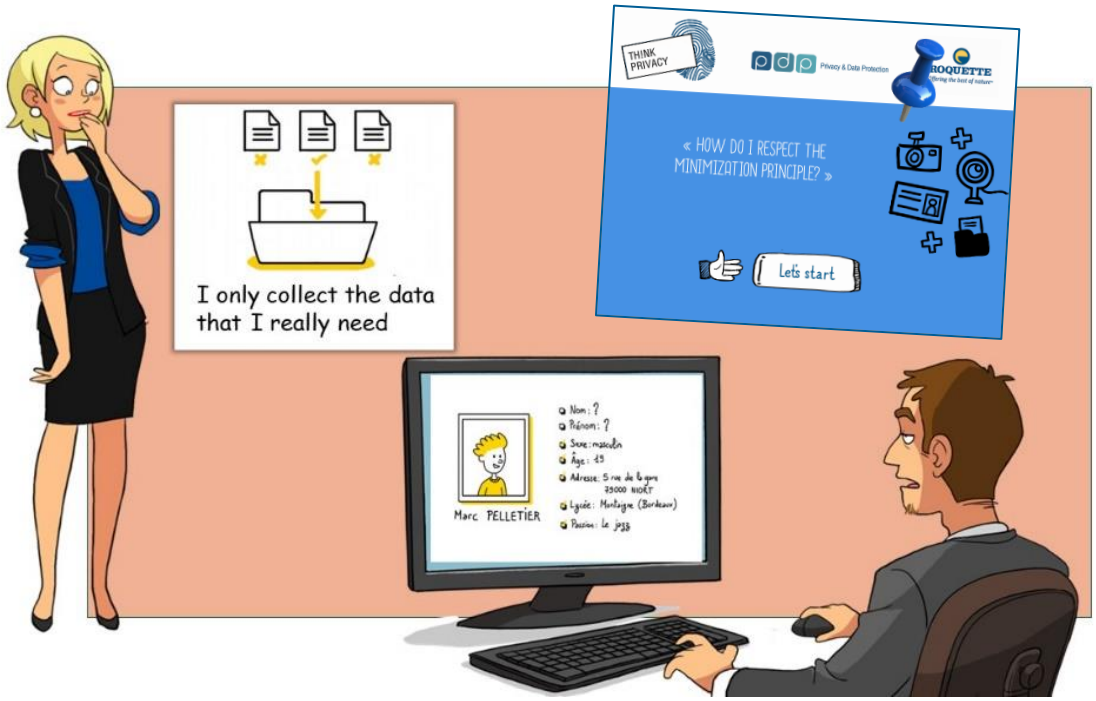
Checklist:

- ☑ Raccogliamo solo dati personali realmente necessari per le finalità specifiche.
- ☑ Disponiamo di dati personali sufficienti a raggiungere in modo appropriato dette finalità.
- ☑ Revisioniamo periodicamente i dati che deteniamo e cancelliamo tutto ciò che non ci serve.
- ☑ Dobbiamo definire la quantità minima di dati personali di cui abbiamo bisogno per raggiungere una determinata finalità. Dobbiamo conservare queste informazioni ma non di più.

Il principio di responsabilità indica la necessità di essere in grado di dimostrare di disporre dei processi appropriati per garantire che vengano raccolti e conservati solo i dati personali necessari.

Va anche tenuto presente che l'GDPR afferma che gli interessati hanno il diritto di completare eventuali dati incompleti che sono non adatti alla finalità, grazie al diritto di rettifica. Hanno anche il diritto di chiedere la cancellazione di dati non necessari per la finalità, grazie al diritto di cancellazione (diritto all'oblio).

Formiamo i nostri dipendenti e miglioriamo i nostri processi interni.



Sicurezza dei dati

La sicurezza informatica è un'attività trasversale la cui implementazione garantisce la condivisione e l'utilizzo dei dati con un livello di protezione adeguato e garantito delle informazioni e delle risorse in questione:

- **Riservatezza**: garantisce che le informazioni siano mantenute riservate e non siano rivelate a persone o entità non appropriate,
- **Integrità**: salvaguarda l'accuratezza e la completezza delle informazioni e dei metodi di trattamento,
- **Disponibilità**: assicura che gli utenti autorizzati abbiano sempre accesso a informazioni, applicazioni e servizi se necessario,
- **Tracciabilità**: fa riferimento alla capacità di tenere tracce pertinenti e, se richiesto, prove di ciò che è stato fatto nel sistema. La tracciabilità è anche inerente a obiettivi legislativi quali non disconoscibilità o responsabilità.

Il patrimonio informativo personale include:

- Documenti cartacei (testi, mappe, foto...),
- Informazioni digitali nell'ambiente d'ufficio,
- Informazioni digitali nell'ambiente mobile,
- Competenze e abilità professionali (detenute da individui o condivise verbalmente),
- Elementi fisici tangibili (quali campioni, ceppi, modelli...).

[DSUG006EN] Gestione della direttiva sulla sicurezza informatica

Pseudonimizzazione indica il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Anonimizzazione è il processo attraverso il quale i dati personali sono alterati in modo tale che l'interessato non possa più essere identificato direttamente o indirettamente, dal **titolare del trattamento** (1) da solo o in collaborazione con un'altra parte.

Crittografia è il metodo attraverso il quale il testo o altri tipi di dati sono convertiti da una forma leggibile a una versione codificata che può essere decodificata solo da un'altra entità che ha accesso a una chiave di decriptazione. La crittografia è uno dei metodi più importanti per garantire la sicurezza dei dati, specialmente in caso di protezione end-to-end dei dati trasmessi attraverso le reti.

(1): Vedere definizione a pagina 38.

Ricordiamo che:

Al fine di mantenere la sicurezza e evitare che il trattamento violi le leggi e i regolamenti sulla protezione dei dati, Roquette e i nostri appaltatori devono valutare i rischi inerenti il trattamento e adottare delle misure per mitigare tali rischi, quali la **crittografia** o la **pseudonimizzazione**.

Le nostre responsabilità:

Dobbiamo adottare delle misure di sicurezza quando trattiamo qualsiasi tipo di dato personale, ma il tipo di misure che adottiamo dipende dalle circostanze specifiche. Dobbiamo garantire la riservatezza, l'integrità e la disponibilità dei sistemi e dei servizi che utilizziamo per il trattamento dei dati personali. Tra le altre cose, ciò può includere le politiche sulla sicurezza delle informazioni, i controlli di accesso, il monitoraggio della sicurezza e i piani di ripristino.

Per tutto il ciclo di vita dei dati personali devono essere adottate misure di sicurezza appropriate e da tutti i soggetti in causa.

Regole	Riferimento Q-Docs	Riferimento GDPR
• Applicare e rivedere le misure di sicurezza definite nella politica di sicurezza e nelle direttive	DDPG007EN Regola 1	Art.32
• Integrazione nei progetti della revisione della sicurezza delle informazioni e della protezione dei dati	DDPG007EN Regola 2	Art.32
• Sicurezza, privacy e protezione dei dati by design e by default	DDPG007EN Regola 3	Art.25
• Integrazione delle clausole di sicurezza delle informazioni e della protezione dei dati con i appaltatori	DDPG007EN Regola 4	Art.32

Formiamo i nostri dipendenti e miglioriamo i nostri processi interni.

Classificazione delle informazioni personali

Il trattamento di dati personali sensibili e di alcune categorie particolari di dati personali è vietato tranne in casi specifici.

Tale trattamento richiede misure protettive in termini di:

Marcatura, accesso, trasmissione, trasporto, copia e stampa, salvataggio e archiviazione, distruzione.

La **Classificazione** mira a identificare il patrimonio informativo sensibile, indipendentemente dalla natura e dal contenitore e specificare, se necessario, misure protettive per ridurre i rischi legati a divulgazione accidentale.

Il livello di **riservatezza della classificazione** è direttamente proporzionale all'impatto stimato di una divulgazione accidentale delle informazioni.

[DSUG001EN] Direttiva sulla protezione delle informazioni

Classificazione della protezione delle informazioni	Tipologie di dati personali	Categorie di dati personali
Livello 1 =ROQUETTE LIMITATO Definizioni: tipo di informazioni per le quali non è consigliata un'ampia divulgazione	Dati personali comuni	Titolo, identità, dati identificativi
		Vita personale (abitudini di vita, stato civile, esclusi dati sensibili)
		Vita professionale (CV, istruzione e formazione professionale, riconoscimenti)
		Informazioni di natura economica e finanziaria (reddito, situazione finanziaria, situazione contributiva)
		Dati di accesso (indirizzi IP, registro eventi)
		Dati di localizzazione (viaggi, dati GPS, dati GSM)
Livello 2 =ROQUETTE RISERVATO Definizioni: tipo di informazioni la cui divulgazione può arrecare danni significativi agli interessi del Gruppo	Dati personali ritenuti sensibili	Numero di previdenza sociale
		Biometrici
		Dati bancari
Livello 3 =ROQUETTE SEGRETO Definizioni: tipo di informazioni la cui divulgazione può danneggiare enormemente gli interessi del Gruppo	Dati personali sensibili ai sensi della Legge sulla protezione dei dati	Orientamenti filosofici, politici, religiosi e sindacali, vita sessuale, dati sanitari, origine razziale o etnica
		Reati, condanne misure di sicurezza

Le nostre responsabilità:

Regole	Riferimento Q-Docs	Riferimento GDPR
• Rispettare i limiti legislativi per il trattamento di dati sensibili	DDPG004EN Regola 1	Art.9
• Vietare il trattamento di dati relativi a condanne penali e reati	DDPG004EN Regola 2	Art.10
• Limitare l'accesso ai dati sanitari solo a personale autorizzato	DDPG004EN Regola 3	Art.9
• Vietare l'uso del numero identificativo nazionale come unico identificatore	DDPG004EN Regola 4	Art.87
• Limitare l'accesso e l'uso di dati bancari	DDPG004EN Regola 5	Art.9
• Limitare l'accesso ai dati sensibili solo al personale autorizzato	DDPG004EN Regola 6	Art.9
• Effettuare una valutazione dell'impatto sulla privacy e gli interessati coinvolti nel trattamento di dati sensibili	DDPG004EN Regola 7	Art.35
• Limitare l'uso di campi di commenti alle informazioni generali	DDPG004EN Regola 8	Buona pratica

Qualche suggerimento pratico...

Esempi di misure di protezione da adottare per ogni categoria di informazioni classificate (cartacea, digitale, know-how, fisica).

Archiviazione dei dati

La crescente necessità di dematerializzare le operazioni e lo scambio di informazioni tra il Gruppo, i clienti e i partner commerciali insieme ai requisiti legislativi e normativi, hanno reso Roquette soggetta a un certo numero di obblighi in termini di lunghezza del periodo di archiviazione dei dati e politiche di gestione dei registri.

Per le sue attività, Roquette acquisisce e tratta una grande quantità di dati sensibili relativi a strategia, risultati finanziari, sviluppo commerciale o impegni, **nonché dati personali relativi a clienti, partner commerciali e membri del personale**.

Le informazioni legate alle attività inviate o ricevute da Roquette devono essere conservate per un periodo minimo, sebbene niente vieti alla società di conservarle in archivio per periodi più lunghi, **tranne nel caso in cui contengano informazioni personali**.

Il limite di tempo, durante il quale le autorità amministrative e competenti possono condurre delle post-ispezioni, varia a seconda della natura delle informazioni da conservare e dei requisiti legislativi pertinenti.

Sono vietati tempi di archiviazione infiniti o indeterminati.

GDPR Art. 5 1. E)

"limitazione della conservazione"

I dati personali saranno conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

I dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato.

Le nostre responsabilità:

- Roquette come titolare del trattamento deve definire tempi di conservazione specifici e appropriati per ciascuna categoria di dati personali raccolti e trattati.
- Prima del trattamento dei dati personali, il titolare dei progetti con l'assistenza del coordinatore della protezione dei dati, deve specificare nel nostro registro la durata di archiviazione dei dati.
- Dobbiamo conservare i dati solo per il tempo necessario per il trattamento e nel rispetto delle leggi applicabili.

Regole	Riferimento Q-Docs	Riferimento GDPR
• Limitare l'archiviazione dei dati al minimo strettamente necessario	DDPG002EN Regola 5	Art. 5 1. E)

A tale proposito Funzioni Globali, GBU e aree sono tenute a conformarsi alle regole di archiviazione delle informazioni della società e a mantenere le procedure associate i condizioni operative.

Esempio:

Al termine di un processo di reclutamento, dobbiamo cancellare le informazioni relative ai candidati che non hanno superato la selezione a meno che essi non acconsentano a rimanere nel nostro "pool" per un tempo limitato (2 anni).

Formiamo i nostri dipendenti e miglioriamo i nostri processi interni.

2 I nostri standard nelle RELAZIONI CON AFFILIATI E APPALTATORI

Ruolo del responsabile e del titolare del trattamento

Titolare del trattamento indica una persona fisica o giuridica, un'autorità pubblica o un altro organismo che, da solo o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali.

Contitolare del trattamento indica due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento. Tuttavia, indipendentemente dalle modalità, ciascun titolare rimane responsabile dell'adempimento degli obblighi stabiliti per i titolari dall'GDPR.

Responsabile del trattamento indica una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che tratta dati personali per conto del titolare del trattamento.

Chi è responsabile del trattamento ai sensi del Regolamento Generale sulla Protezione dei Dati?

(Articolo 4 dell'GDPR – Definizioni).

Moltissimi provider di servizi possono avere lo status di responsabile del trattamento nel senso legale del termine. Le attività di un responsabile del trattamento possono riguardare un compito molto specifico (sub-contratto della distribuzione della corrispondenza) o essere più generali e a ampio raggio (gestione di un intero servizio per conto di un'altra organizzazione, quale ad esempio la gestione degli stipendi dei dipendenti).

I seguenti soggetti rientrano in particolare nell'ambito di applicazione dell'GDPR:

- I provider di servizi IT (hosting, manutenzione, ecc.), gli integratori di software, le società di sicurezza informatica o le società di consulenza IT (note in passato come società fornitrici di servizi di ingegneria IT) che hanno accesso ai dati,
- agenzie di marketing o di comunicazione che trattano dati personali per conto dei clienti e
- più in generale, qualsiasi organizzazione che fornisce un servizio che comporta il trattamento di dati personali per conto di un'altra organizzazione,
- anche un'autorità pubblica o un'associazione possono essere considerate tali.

Gli sviluppatori di software e i produttori di dispositivi (quali terminali per la timbratura, attrezzature biometriche o dispositivi medici) non rientrano nell'ambito di applicazione del Regolamento se non hanno accesso ai dati personali o non si occupano del loro trattamento.

Esempio di ruolo del responsabile e del titolare del trattamento:

La società A offre un servizio di consegna della corrispondenza di marketing utilizzando i file di dati delle società B e C.

La società A è un responsabile del trattamento per le società B e C nella misura in cui tratta i dati dei clienti necessari per l'invio della corrispondenza per conto o in base alle disposizioni delle società B e C.

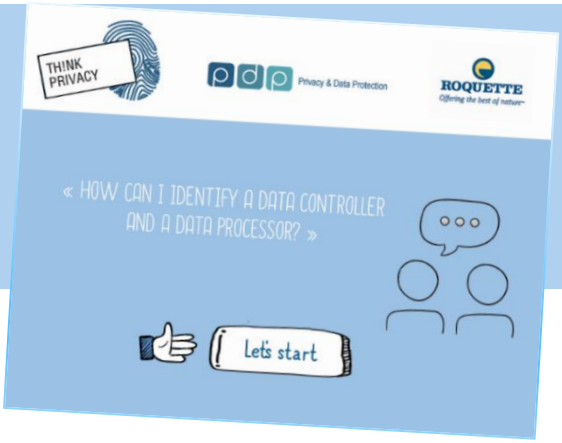
Le società B e C sono i titolari della gestione dei clienti, anche per quanto riguarda la consegna della corrispondenza di marketing.

La società A ha anche il ruolo di titolare del trattamento relativamente alla gestione del personale che impiega e la gestione dei suoi clienti che include le società B e C.

Testo ufficiale

- Articolo 4 dell'GDPR per le definizioni di titolare e responsabile del trattamento
- Articolo 28.10 dell'GDPR per la nozione di titolare del trattamento

Formiamo i nostri dipendenti e miglioriamo i nostri processi interni.



Clausole di protezione dei dati

Quando è necessario un contratto e perché è importante?

Ogniqualvolta, in qualità di titolare del trattamento, utilizziamo un processore che tratta i dati personali per nostro conto, tra le parti deve essere stipulato un contratto scritto.
Il contratto è importante perché entrambe le parti comprendano le loro responsabilità e i loro obblighi.

I contratti contenenti clausole di protezione dei dati specifiche e/o contratti di protezione dei dati tra Roquette, in qualità di titolare, e i suoi processori garantiscono la comprensione da parte di entrambi di obblighi e responsabilità. I contratti ci aiutano anche a conformarci all'GDPR e ci assistono nel dimostrare ai singoli individui e alle autorità competenti il rispetto della conformità come richiesto dal principio di responsabilità.

Quali responsabilità e obblighi abbiamo in qualità di titolare del trattamento quando ci avvaliamo di un processore?

Dobbiamo utilizzare solo processori in grado di fornire garanzie sufficienti in merito all'adozione di misure tecniche e organizzative appropriate che garantiscano che il trattamento sarà conforme ai requisiti dell'GDPR e proteggerà i diritti degli interessati.

In qualità di titolare del trattamento siamo in primo luogo responsabili del totale rispetto dell'GDPR e delle altre leggi sulla privacy dei dati in vigore e del fatto di poter dimostrare tale conformità. In caso contrario, siamo tenuti al risarcimento dei danni dei procedimenti giudiziari o siamo soggetti a multe, altre sanzioni o misure correttive.

Cosa cambia con l'GDPR?

L'GDPR rende i contratti scritti tra titolari e processori un obbligo piuttosto che un modo di dimostrare la conformità con il principio di protezione dei dati (misure di sicurezza appropriate) ai sensi delle leggi sulla protezione dei dati in vigore.

Ora questi contratti devono includere condizioni minime specifiche. Queste condizioni sono pensate per garantire che il trattamento realizzato da un processore soddisfi tutti i requisiti dell'GDPR, non solo quelli relativi alla sicurezza dei dati personali.

Regola	Riferimento Q-Docs	Riferimento GDPR
• Integrazione di clausole relative alla sicurezza delle informazioni e alla protezione dei dati con i appaltatori	DDPG007EN Regola 4	Art. 32
• Sicurezza dei contraenti	DSUG016EN	

Cosa è necessario inserire nel contratto?

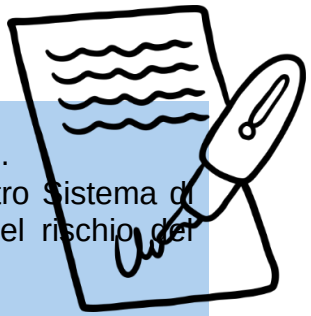
Nei contratti devono essere enunciati:

- ☑ l'oggetto e la durata del trattamento;
- ☑ la natura e la finalità del trattamento;
- ☑ il tipo di dati personali e le categorie di interessati; e
- ☑ gli obblighi e i diritti del titolare del trattamento.

I contratti devono inoltre includere condizioni e clausole specifici riguardanti:

- ☑ trattamento solo sulla base delle istruzioni documentate del titolare del trattamento;
- ☑ l'obbligo di riservatezza;
- ☑ misure di sicurezza appropriate;
- ☑ utilizzo di sub-processori;
- ☑ diritti degli interessati;
- ☑ offrire assistenza al titolare del trattamento;
- ☑ disposizioni di un contratto end-to-end; e
- ☑ verifiche e ispezioni.

Formiamo i nostri dipendenti e miglioriamo i nostri processi interni.



- Guida sulla protezione dei dati per sub-contratto conforme all'GDPR.
- Modello di clausole contrattuali di sub-contratto disponibili nel nostro Sistema di gestione della privacy: OneTrust@Roquette> Modulo Gestione del rischio del fornitore.

Consenso al trasferimento dei dati

Un **Trasferimento di dati** è qualsiasi comunicazione, copia o transito di dati personali (quali server di hosting, invio di allegati per e-mail, strumenti di accesso remoto, condivisione dello schermo, ecc.) destinata al trattamento in altri paesi che non dispongono delle stesse leggi in materia di protezione dei dati personali.

Siamo più connessi che mai. Per Roquette, che opera su scala mondiale, il trasferimento dei dati rappresenta un elemento essenziale delle attività quotidiane. Roquette, ad esempio, archivia i dati personali dei dipendenti in un servizio cloud ospitato all'estero e condivide i dati personali di dipendenti e clienti con le sue filiali in tutto il mondo.

In che misura l'GDPR e le altre leggi sulla protezione dei dati in vigore influiscono su questi trasferimenti di dati internazionali?

Le nostre responsabilità:

Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale ha luogo soltanto se:

- La legislazione locale lo consente e/o l'autorità di vigilanza ha deciso che il paese terzo, un territorio o uno o più settori specificati all'interno di quel paese terzo o l'organizzazione internazionale in questione garantiscono un adeguato livello di protezione o hanno dato la loro autorizzazione e/o
- Sia adottata una misura legislativa (ad es.: Norme vincolanti d'impresa o clausole contrattuali standard per il trasferimento dei dati personali al processore stabilito in un paese terzo ai sensi della Direttiva 95/46/CE del Parlamento europeo e del Consiglio, ecc.).

Regola	Riferimento Q-Docs	Riferimento GDPR
• Adottare le misure per il trasferimento dei dati personali a paesi terzi o organizzazioni internazionali	DDPG002EN Regola 6	Art. da 44 a 50

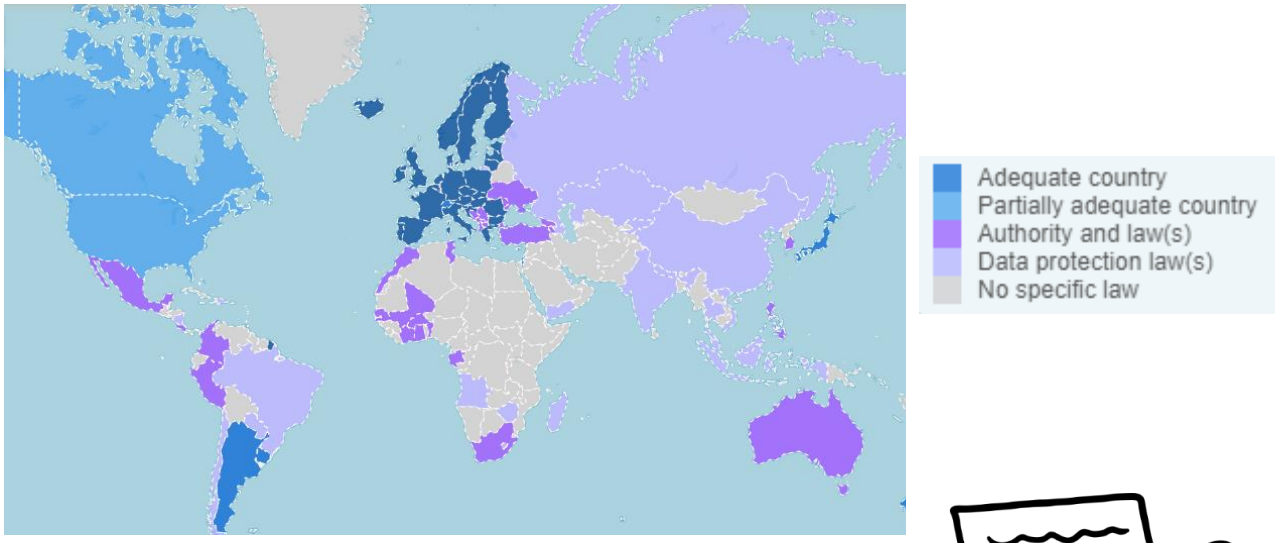
In ogni caso contattare prima il DPO.

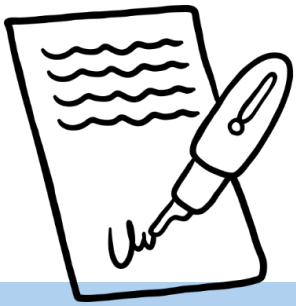
In quale paese posso trasferire i dati personali e a quali condizioni?

Per una panoramica, consultare questa mappa:

https://www.cnil.fr/en/data-protection-around-the-world.

Questa mappa vi permette di vedere il livello di protezione dei dati in ciascun paese.





Formiamo i nostri dipendenti e miglioriamo i nostri processi interni.

- Sezione del Contratto di trasferimento dei dati, compreso nel nostro modello di Contratto di trattamento dei dati.
- FAQ per chiarire alcune questioni sollevate in seguito all'entrata in vigore della decisione della Commissione europea sulle clausole contrattuali standard per il trasferimento dei dati personali ai processori stabiliti in paesi terzi.

3 I nostri standard nelle RELAZIONI CON la nostra RETE E LE AUTORITÀ DI CONTROLLO

Data Protection Officer

Il Gruppo ha nominato un Responsabile della protezione dei dati – Data Protection Officer.

Il Responsabile della protezione dei dati (Data Protection Officer) o DPO ci assiste nel monitorare la conformità interna, ci informa e ci fornisce consigli sugli obblighi relativi alla protezione dei dati, fornisce pareri sulla Valutazione dell'impatto della protezione dei dati (DPIA) e agisce come punto di contatto per gli interessati e le autorità di controllo.

Il DPO deve essere indipendente, esperto nella protezione dei dati, disporre delle risorse adeguate e riferisce ai livelli dirigenziali più elevati.

Il DPO ci aiuta a dimostrare la compliance e è un soggetto della maggiore attenzione sulla responsabilità.

Compiti del DPO	Riferimento Q-Docs	Riferimento GDPR
• Il nostro DPO ha il compito di monitorare la conformità con l'GDPR e altre leggi sulla protezione dei dati, le politiche di protezione dei dati, la sensibilizzazione, la formazione e le verifiche	MDPG001EN Manuale sulla protezione dei dati personali	GDPR Articolo 39 Compiti del Responsabile della Protezione dei Dati – Data Protection Officer
• Terremo conto del parere del DPO e delle informazioni che fornisce sugli obblighi di protezione dei dati		
• Quando realizziamo una DPIA, sentiamo il parere del DPO che monitora anche il processo		
• Il DPO agisce come punto di contatto per le autorità di controllo		
• Nello svolgimento dei suoi compiti, il DPO tiene in debito conto il rischio associato alle attività di trattamento e tiene conto della natura, dell'ambito, del contesto e delle finalità del trattamento		

Il DPO del Gruppo è stato designato al CNIL dal CEO e ha assunto il suo ruolo il 25 maggio 2018, data di applicazione dell'GDPR.

Disponibilità del DPO:

- La nostra Responsabile della protezione dei dati (Data Protection Officer), Jennifer Godin, è facilmente raggiungibile come punto di contatto per dipendenti, individui e autorità di controllo.

- Abbiamo pubblicato i recapiti del DPO e li abbiamo comunicati alle autorità di controllo.

  - ☑ https://www.Roquette.com/data-protection
  - ☑ ONE > Funzioni Globali > Protezione dei dati
  - ☑ ONE > Community > Rete di protezione dei dati

Contattate il DPO in caso di:

- ☑ Trattamento dei dati personali
- ☑ Richieste delle persone interessate
- ☑ Violazione dei dati personali
- ☑ Necessità di consulenza o assistenza

Un singolo punto di contatto: dpo@Roquette.com o jennifer.godin@Roquette.com

Formiamo i nostri dipendenti e miglioriamo i nostri processi interni.

Rete di protezione dei dati

Esiste una rete di collegamenti negli uffici e di DPO locali o coordinatori che permette al Responsabile della protezione dei dati del Gruppo (Data Protection Officer) rispettivamente di attuare le regole di protezione dei dati personali in ciascuna business unit e di supportare i vari uffici, e di conformarsi ai requisiti delle legislazioni e dei regolamenti pertinenti in materia di protezione dei dati nel paesi nei quali il Gruppo opera.

I DPO/Coordinatori locali avranno i seguenti compiti:

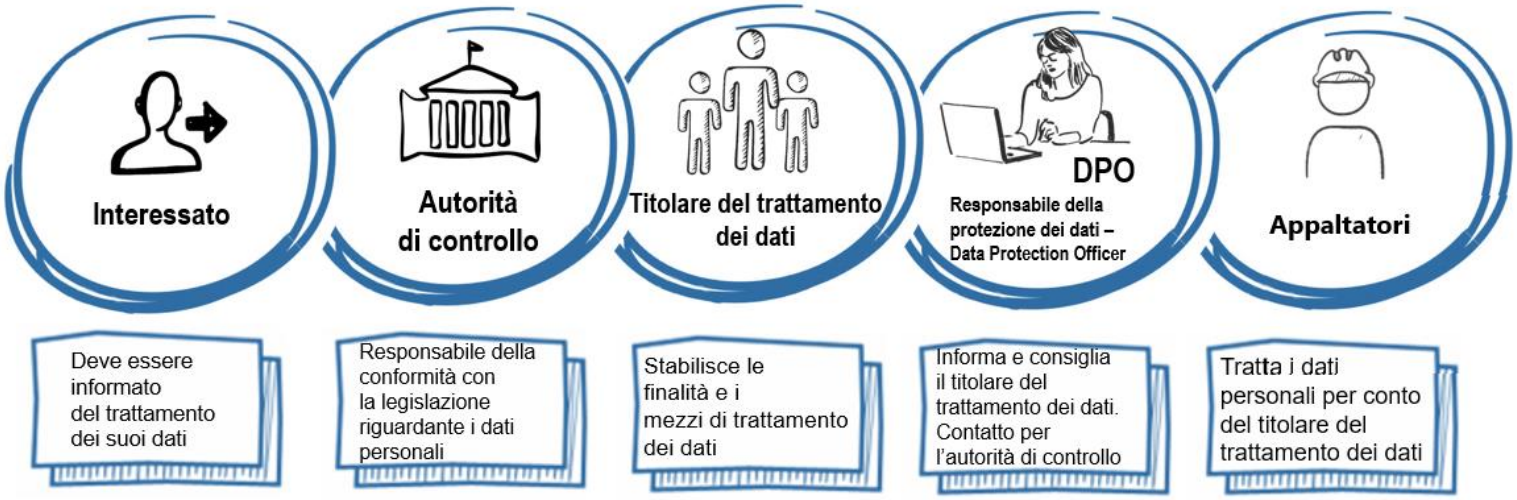
- Informare e fornire consulenza sugli obblighi contenuti nella Politica di protezione di dati personali di Roquette definiti dal DPO del Gruppo di Roquette e sui requisiti delle leggi locali applicabili in materia di protezione dei dati;
- Monitorare il rispetto della legislazione locale, di altre legislazioni e dei regolamenti applicabili in materia di protezione dei dati, quando richiesto, con l'assistenza del DPO del Gruppo di Roquette e il rispetto delle politiche relative alla protezione dei dati personali;
- Fornire consulenza a livello locale se richiesto sull'impatto della valutazione della protezione dei dati e monitorarne la performance;
- Cooperare con le autorità di controllo locali;
- Agire come punto di contatto per il DPO del Gruppo di Roquette su questioni relative al trattamento e consultare il DPO del Gruppo di Roquette, se opportuno, su altre questioni;
- Riferire le proprie attività al DPO del Gruppo di Roquette per contribuire al sistema di gestione di protezione dei dati.

Formiamo i nostri dipendenti e miglioriamo i nostri processi interni

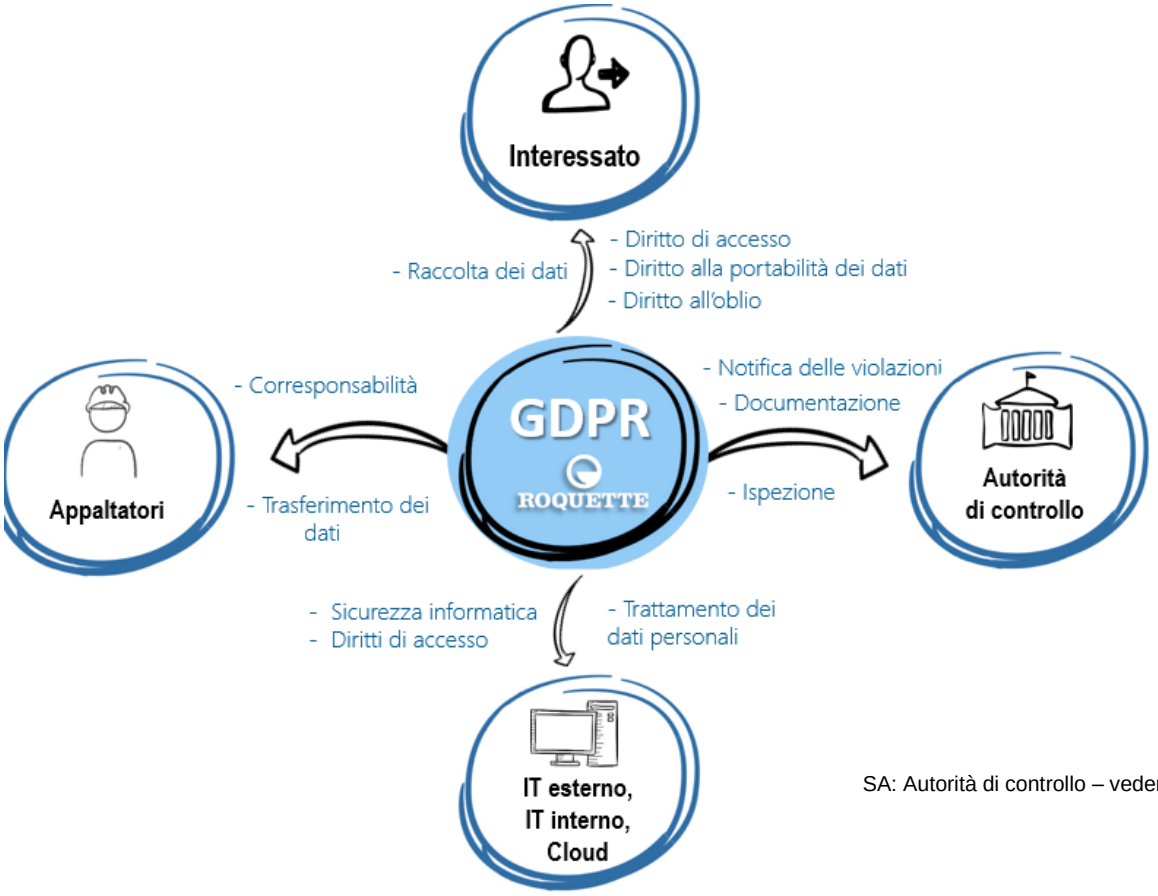
Il nostro seminario annuale sulla PDP è il luogo di incontro della nostra rete di collaboratori per la protezione dei dati e della privacy.

e soggetti interessati

Chi sono i nuovi attori?



Quali sono le relazioni tra questi soggetti interessati?



SA: Autorità di controllo – vedere pagina 50

Autorità di controllo

Nel mondo molti paesi hanno una legislazione sulla protezione dei dati e un'Autorità garante della protezione dei dati (DPA) indipendente.
Queste autorità sono le autorità di regolamentazione nazionale indipendenti per la privacy e la libertà d'informazione. Promuove e tutela i diritti degli interessati ad avere accesso alle informazioni conservate dalle organizzazioni e alla protezione delle loro informazioni personali.

Che ruolo svolge l'Autorità di Controllo nel contesto dell'GDPR?

Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di controllare l'applicazione delle leggi sui dati personali e la privacy al fine di tutelare i diritti e le libertà fondamentali degli interessati con riguardo al trattamento dei dati e di agevolare la libera circolazione dei dati personali all'interno dell'Unione.

Nell'ambito dell'GDPR tutti gli Stati membri dell'UE hanno un'autorità garante della protezione dei dati che in genere serve da punto di contatto principale per i soggetti interessati all'interno dello Stato membro.

Per essere certi della coerente applicazione dell'GDPR in tutta l'UE, ogni autorità di controllo coopera con le altre e con la Commissione europea.

Ogni autorità di controllo sul proprio territorio è tenuta a promuovere la consapevolezza e favorire la comprensione di rischi, norme, garanzie e diritti in relazione al trattamento dei dati personali.

Ha anche il potere di intentare un'azione in caso di violazione della legislazione sulla protezione dei dati e di offrire consulenza su questioni specifiche e/o assistenza dalla prospettiva delle organizzazioni.

In breve, le responsabilità delle Autorità di controllo (SA) sono di:

- Garantire l'applicazione delle norme incluse le ammende,
- Chiarire l'applicazione delle norme, se necessario, ad es. attraverso linee guida,
- Promuovere una cultura di dialogo con tutti i soggetti interessati, incluse le aziende,
- Cooperare.

CNIL: Commissione nazionale dell'informatica e delle libertà - DPA francese.

Autorità di controllo capofila

- L'autorità di controllo dello stabilimento principale o del titolare del trattamento o del processore è competente ad agire in qualità di autorità di controllo capofila. Deve collaborare con le altre autorità interessate.

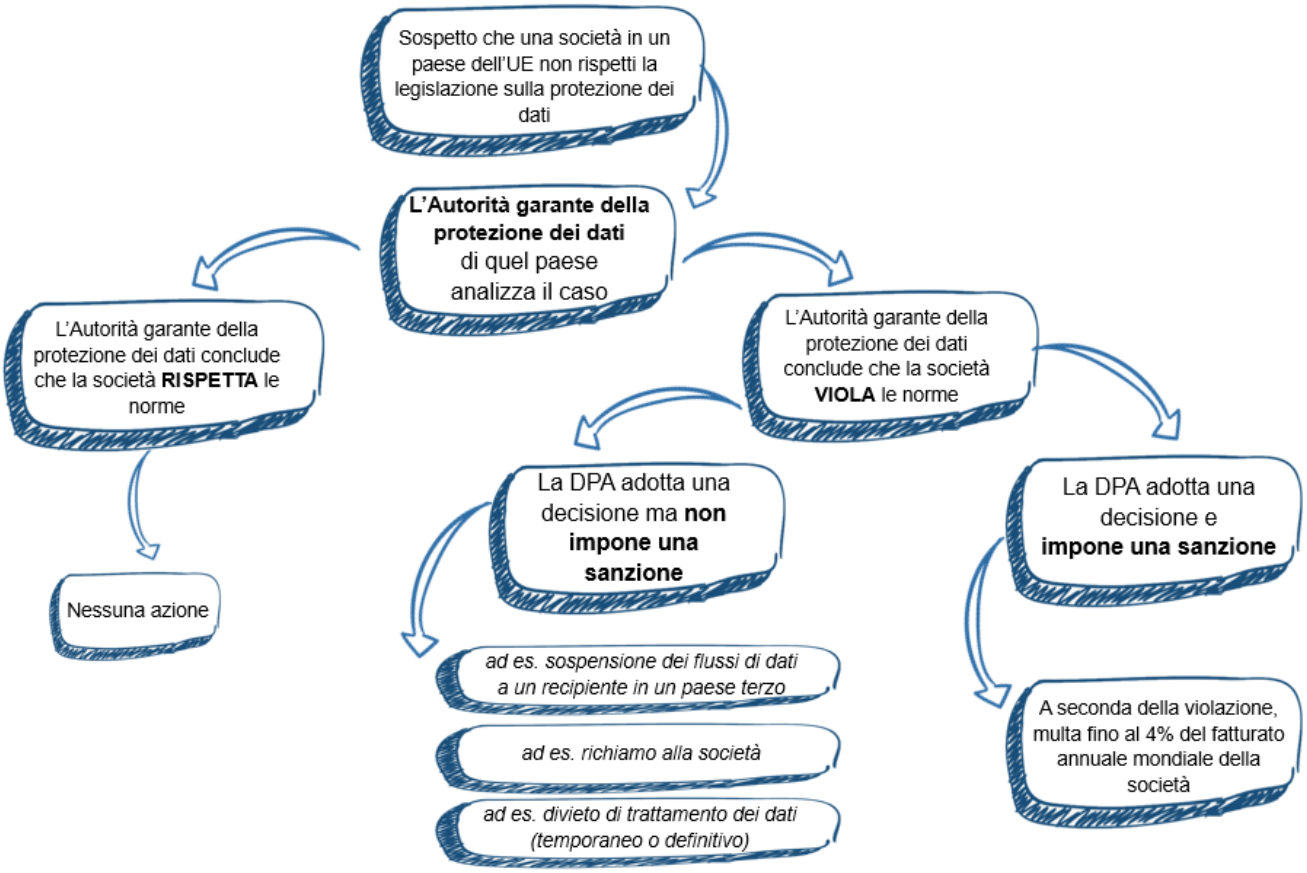
- Identificare un'autorità di controllo capofila è pertinente solo quanto un titolare o un processore realizza un trattamento transfrontalieri dei dati personali.

Come identificare "l'autorità di controllo capofila"?

Individuare la sede del titolare del trattamento principale dell'amministrazione centrale nell'UE.
L'autorità di controllo del paese nel quale si trova la sede dell'amministrazione centrale è l'autorità di controllo capofila del titolare del trattamento.

La ***CNIL*** *è l'autorità di controllo capofila di Roquette*

Come funziona il meccanismo sanzionatorio dell'GDPR in pratica?



Governance

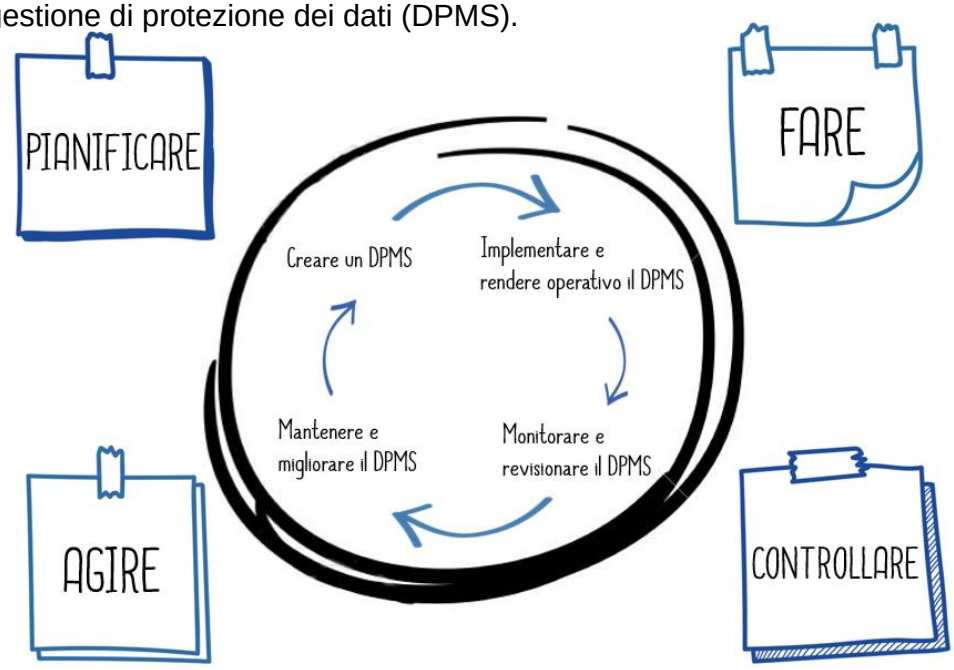
"L'**organizzazione di protezione dei dati** è strutturata principalmente intorno al Responsabile della protezione dei dati (Data Protection Officer), ai suoi coordinatori per sede e per funzione, al Chief Executive Officer che agisce come Titolare dei dati, agli Head of Global Functions che sono responsabili dell'attuazione del trattamento dei dati personali e ai subappaltatori in qualità di Processori." [MDPG001EN]

Adottiamo un approccio per processo per definire, implementare, gestire, monitorare, revisionare, mantenere e migliorare il Personal **D**ata **P**rotection **M**anagement **S**ystem (**DPMS - Sistema di gestione di protezione dei dati personali**) di Roquette.

Il processo e l'approccio alla gestione della protezione dei dati personali definito in questa governance incoraggia gli utenti a porre l'accento sull'importanza di:

1) conoscere i requisiti in materia di protezione dei dati di Roquette e la necessità di definire direttive e procedure per la protezione dei dati;
2) attuare e rendere operativi i controlli per gestire i legati alla protezione dei dati di Roquette nel contesto dei rischi commerciali di natura generale di Roquette;
3) monitorare e rivedere la performance e l'efficacia dei DPM; e
4) migliorare di continuo sulla base di misurazioni oggettive.

Adottiamo il modello "Plan-Do-Check-Act" (PDCA) che è applicato per strutturare tutti i processi del sistema di gestione di protezione dei dati (DPMS).



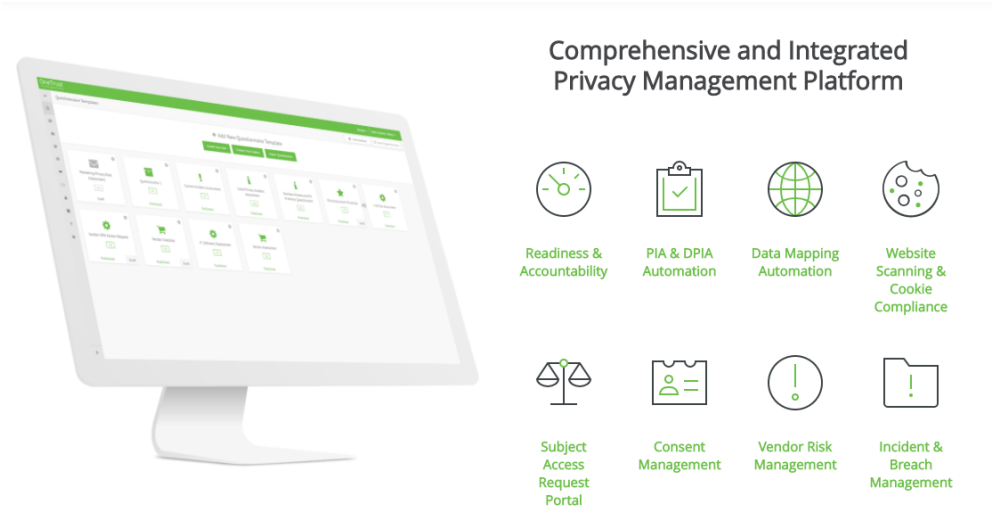
Il nostro approccio:

Il nostro programma di conformità GDPR prevede:

- La comprensione di come un'organizzazione raccoglie, memorizza, utilizza e trasferisce i dati per garantire la conformità,
- La creazione della cultura della conformità all'interno di un'organizzazione,
- La realizzazione di valutazioni dell'impatto sulla privacy,
- La preparazione a eventuali violazioni dei dati,
- La distribuzione delle risorse per il programma di privacy,
- L'implementazione di un sistema di gestione di protezione dei dati (Plan – Do – Check – Act).

Per raggiungere questi obiettivi, come parte del nostro programma abbiamo:

- Definito una Politica di protezione dei dati e associato governance e documentazione,
- Gestito un progetto di conformità GDPR per la revisione del trattamento, la gestione delle violazioni dei dati, la revisione dei contratti, le clausole sulla protezione dei dati, il contratto sul trasferimento dei dati, ecc.,
- Implementato un software di gestione della privacy conforme all'GDPR.



Le principali caratteristiche di questa piattaforma di gestione sono:

- Manutenzione del registro di trattamento dei dati (mappatura dei dati),
- Gestione del rischio associata al trattamento (dal PIA, ecc.),
- Gestione di richieste e diritti (accesso, rettifica, opposizione, ecc.),
- Gestione di incidenti e violazioni dei dati,
- Gestione della documentazione di conformità.

Responsabilità

La **Responsabilità** è uno dei principi della protezione dei dati. Ci rende responsabili del rispetto dell'GDPR e afferma che dobbiamo essere in grado di dimostrare la compliance.

Perché la responsabilità è importante?

Assumersi la responsabilità di quello che facciamo con i dati personali e dimostrare le cose che abbiamo fatto per proteggere i diritti delle persone non solo ci permette una conformità giuridica, ci offre anche un vantaggio competitivo. La responsabilità rappresenta una reale opportunità per mostrare e dimostrare in che modo rispettiamo la privacy delle persone. Ciò può essere utile per accrescere e mantenere la fiducia delle persone.

Inoltre, se qualcosa va storto, essere in grado di mostrare che abbiamo attivamente considerato i rischi e adottato misure e garanzie può aiutarci a garantire l'attenuazione di eventuali misure coercitive potenziali. D'altro canto, la mancata adozione di buone pratiche per la protezione dei dati può esporci a sanzioni e a un danno d'immagine.

Cosa significa in concreto aderire al principio di responsabilità?

Il trattamento dei dati personali comporta un obbligo di diligenza e l'adozione di misure pratiche e concrete per la loro protezione. Aderire al principio di responsabilità significa:

- documentare e comunicare nel modo appropriato tutte le direttive, le procedure e le pratiche relativa alla privacy (la nostra "Policy");
- assegnare a un individuo specifico all'interno dell'organizzazione (che a sua volta può delegare a altri all'interno dell'organizzazione ove opportuno) il compito di attuare la Politica;
- quando si trasferiscono dati personali a un terzo, assicurarsi che il destinatario sia tenuto a rispettare un livello equivalente di Privacy e protezione dei dati attraverso mezzi contrattuali o altri mezzi quali politiche interne vincolanti (la legislazione applicabile può contenere altri requisiti riguardanti i trasferimenti di dati internazionali);
- fornire una formazione adeguata al personale del titolare dei dati che avrà accesso ai dati personali;
- definire procedure efficienti per la gestione di reclami interni e per il ricorso da parte degli interessati in merito all'uso dei dati personali;

- informare gli interessati di violazioni della privacy che possono comportare danni sostanziali per loro (a meno che sia proibito, ad es. quando si collabora con le autorità preposte all'applicazione della legge) e delle misure adottate per risolvere il problema;
- notificare a tutti gli interlocutori in materia di privacy le violazioni della privacy come richiesto in alcune giurisdizioni (ad es. le autorità per la protezione dei dati) e in relazione al livello di rischio;
- consentire l'accesso all'interessato che è parte lesa a misure e/o mezzi di ricorso appropriati e efficaci, quali la rettifica, la cancellazione o la restituzione in caso di violazione della Privacy; e
- valutare procedure di risarcimento nei casi in cui è difficile o impossibile riportare allo stato originale la privacy della persona fisica come se nulla fosse accaduto.

Checklist:

- ☑ Abbiamo la responsabilità di rispettare l'GDPR a tutti i livelli dell'organizzazione, compresi i vertici dell'azienda.
- ☑ Conserviamo le prove delle azioni intraprese per conformarci all'GDPR.

Adottiamo misure tecniche e organizzative appropriate, quali:

- ☑ adottare a attuare norme per la protezione dei dati;
- ☑ adottando un approccio alla 'protezione dei dati by design e by default' - adottando misure di protezione dei dati appropriate nell'intero ciclo di vita delle operazioni di trattamento;
- ☑ stipulando contratti scritti con le organizzazioni che trattano i dati personali per nostro conto;
- ☑ conservando la documentazione delle attività di trattamento;
- ☑ adottando misure di sicurezza appropriate;
- ☑ registrando e, se necessario, riferendo violazioni dei dati personali;
- ☑ effettuando valutazioni dell'impatto della protezione dei dati quando si utilizzano dati personali che possono comportare rischi elevati per gli interessi dei soggetti;
- ☑ nominando un responsabile della protezione dei dati; e
- ☑ aderendo ai codici di condotta pertinenti e sottoscrivendo documenti di certificazione (laddove possibile).

- ☑ Rivediamo e aggiorniamo le misure relative alla responsabilità a intervalli appropriati.

Documentazione

Cosa si intende per documentazione?

Siamo tenuti a conservare una registrazione delle attività di trattamento che riguarda aree quali le finalità del trattamento, la condivisione e l'archiviazione dei dati; questo è ciò che definiamo **documentazione**.

Documentare le attività di trattamento è importante, non solo perché è un requisito legislativo, ma anche perché contribuisce alla buona governance dei dati e ci aiuta a dimostrare la conformità a altri aspetti dell'GDPR e alla legislazione vigente in materia di protezione dei dati.

Checklist:

Documentazione delle attività di trattamento - requisiti

- ☑ In qualità di titolare del trattamento dei dati personali, documentiamo tutte le informazioni pertinenti ai sensi dell'Articolo 30(1) dell'GDPR.
- ☑ Documentiamo le attività di trattamento per iscritto.
- ☑ Documentiamo le attività di trattamento in modo granulare con collegamenti significativi tra le varie informazioni.
- ☑ Procediamo a revisioni regolari dei dati personali che trattiamo e aggiorniamo la documentazione di conseguenza.

Documentazione delle attività di trattamento - buone pratiche

- ☑ Documentiamo le attività di trattamento in formato digitale in modo tale da poter aggiungere, eliminare e modificare facilmente le informazioni.

Nel preparare la documentazione delle attività di trattamento:

- ☑ teniamo verifiche informative per analizzare quali sono i dati conservati dall'organizzazione;
- ☑ utilizziamo questionari attraverso gli strumenti Digitali, Sicurezza e Privacy di cui disponiamo e parliamo con il personale dell'organizzazione per avere un quadro più completo delle attività di trattamento; e
- ☑ rivediamo politiche, direttive, procedure, contratti e accordi in ambiti quali archiviazione, sicurezza e condivisione di dati.

Come parte della registrazione delle attività di trattamento documentiamo o inseriamo nella documentazione:

- ☑ informazioni richieste per l'informativa sulla privacy;
- ☑ registrazione del consenso, se richiesta;
- ☑ contratti titolare-processore;
- ☑ localizzazione dei dati personali;
- ☑ Rapporti sulla valutazione dell'impatto della protezione dei dati; e anche
- ☑ registrazioni di violazioni dei dati personali;
- ☑ registrazioni di richieste degli interessati.

Dove si trova la documentazione sulla protezione dei dati?

ONE
Funzione globale
Protezione dei dati

Privacy & Data Protection

La protezione dei dati è di importanza cruciale per tutti all'interno della nostra organizzazione"

Contenuto

- Leggi e regolamenti
- Informazione e sensibilizzazione
- Buone pratiche e politiche

ONE
Community
Rete di protezione dei dati

Data Protection Network

"Siamo tutti attori nella protezione dei dati personali"

Contenuto

- Politica sulla protezione dei dati personali
- Sistema di gestione della protezione dei dati
- Legislazione locale
- Risorse umane
- Global Digital
- Legal & Compliance
- Verifica e controllo interno
- GBU & Commerciale
- Innovation, R&D
- Global Security
- Insurance & Risk Management

OneTrust
Software di gestione della privacy

OneTrust
Privacy Management Software
@ ROQUETTE

"Lo strumento di gestione della Privacy dedicato a sicurezza della privacy e rischi di terze parti"

Moduli

Data Mapping Automation

PIA & DPIA Automation

Subject Access Request Portal

Incident & Breach Management

CULTURA → CONFORMITÀ → RESPONSABILITÀ

Valutazione dell'impatto sulla privacy

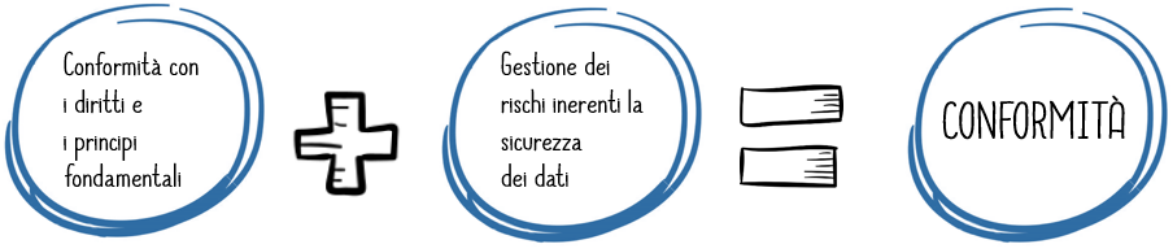
La **Valutazione dell'impatto sulla Privacy** o **PIA** è un processo per descrivere il trattamento, valutarne la necessità e la proporzionalità e contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche risultanti dal trattamento dei dati personali valutandoli e determinando le misure da adottare.

L'acronimo "**PIA**" è utilizzato in modo intercambiabile in riferimento alla **Valutazione dell'impatto sulla Privacy** e alla **Valutazione dell'impatto sulla protezione dei dati** (**DPIA**).

Come si conduce una PIA?

L'approccio di conformità realizzato attraverso una PIA si basa su due pilastri:

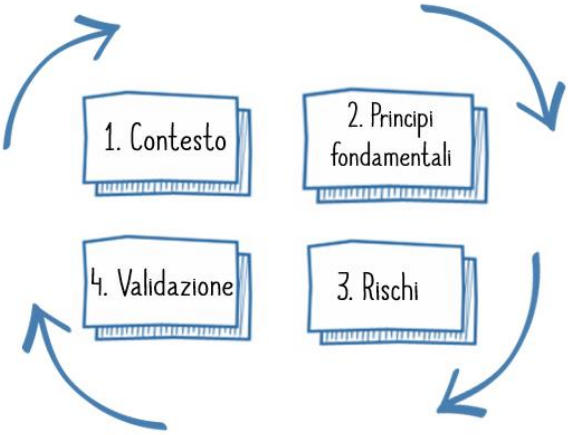
1) **diritti e principi fondamentali**, che sono "non negoziabili", stabiliti dalla legge e che devono essere rispettati, indipendentemente dalla natura, dalla gravità e dalla probabilità dei rischi;
2) la **gestione dei rischi per la Privacy dell'interessato**, che determina i controlli tecnici e organizzativi appropriati per proteggere i dati personali.



Approccio di conformità utilizzando una PIA

Riassumendo, per effettuare una PIA è necessario:

1) definire e descrivere il contesto del trattamento dei dati personali in questione;
2) analizzare i controlli che garantiscono la conformità con i principi fondamentali: la proporzionalità e la necessità del trattamento e la protezione dei diritti degli interessati;
3) valutare i rischi per la privacy associati alla sicurezza dei dati e garantire che siano presi adeguatamente in considerazione;
4) documentare formalmente la validazione della PIA alla luce dei fatti precedenti o decidere di rivedere le fasi precedenti.



Approccio generale per effettuare una PIA

Si tratta di un processo di miglioramento continuo. Pertanto, a volte sono necessarie varie interazioni per ottenere un sistema di protezione della privacy accettabile. Richiede anche il monitoraggio delle modifiche nel tempo (contesto, controlli, rischi, ecc.), ad esempio ogni anno e un aggiornamento ogniqualvolta interviene una modifica significativa.

L'approccio deve essere implementato non appena viene concepito un nuovo trattamento dei dati personali. Attuare subito questo tipo di approccio rende possibile determinare i controlli necessari e sufficienti e perciò ottimizzare i costi. Al contrario, attuare questo approccio dopo la creazione del sistema e la definizione dei controlli può rimettere in discussione le scelte fatte.

Le nostre responsabilità:

- Quando un tipo di trattamento in particolare che si avvale di nuove tecnologie e prende in considerazione la natura, l'ambito, il contesto e le finalità del trattamento, potrebbe comportare un rischio elevato in termini di diritti e libertà delle persone fisiche, Roquette in qualità di titolare del trattamento, prima del trattamento, procederà a effettuare una valutazione dell'impatto delle operazioni di trattamento sulla protezione dei dati personali.
- Il titolare del progetto chiederà il parere del Data Protection Officer (Responsabile della protezione dei dati) designato quando effettua una valutazione dell'impatto sulla protezione dei dati.

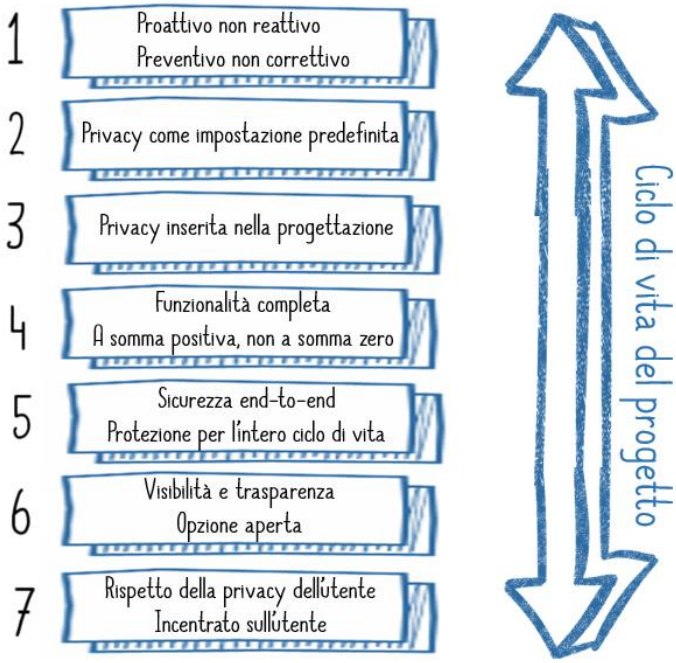
Regole	Riferimento Q-Docs	Riferimento GDPR
• Effettuare una PIA in caso di rischio elevato	DDPG003EN Regola 1	Art. 35
• Contenuto di una PIA	DDPG003EN Regola 2	
• Compiti del DPO relativamente alla PIA	DDPG003EN Regola 3	
• Revisione della PIA	DDPG003EN Regola 4	

We train our employees and improve our internal processes.

- Linee guida su Community Rete protezione dati.
- Formazione su Workday Learning.
- CNIL Metodologia PIA, edizione febbraio 2018 - https://www.cnil.fr/en/home.

Privacy by Design e by Default

Privacy by Design significa mettere in atto misure relative alla privacy nella progettazione, attuazione e gestione di un determinato sistema, processo aziendale o specifiche di progetto.



Cosa s'intende per Protezione dei dati by Design?

La legislazione sulla protezione dei dati contiene i principi basilari per la tutela della privacy degli interessati.

La protezione dei dati by design e by default contribuisce a essere certi che i sistemi informatici utilizzati rispettino i principi di protezione dei dati e che i sistemi tutelino i diritto degli interessati.

Ricordiamo che:

Roquette utilizza sistemi informatici e database per una vasta gamma di compiti operativi e amministrativi. Gran parte di questi sistemi informatici trattano dati personali, per cui è di cruciale importanza che siano pienamente conformi al regolamento.

Le aziende che prendono in seria considerazione le questioni relative alla protezione dei dati, generano fiducia.

Pertanto, l'adozione di forti misure per la protezione dei dati può rappresentare un vantaggio competitivo.

L'impegno da parte della dirigenza è di cruciale importanza nell'adozione della decisione di applicare i principi della protezione dei dati by design nella scelta dei fornitori e nello sviluppo di software.

La dirigenza deve anche garantire risorse sufficienti per questa attività.

Tenere in considerazione la protezione dei dati durante tutto il processo di sviluppo è sia vantaggioso in termini di costi e più efficiente rispetto a apportare delle modifiche a parte di un software già esistente.

Le nostre responsabilità:

Con l'GDPR, la protezione dei dati by design è divenuta per la prima volta un obbligo giuridico. Ciò significa che la protezione dei dati e la Privacy devono essere considerate fin dalla progettazione delle specifiche e dell'architettura dei sistemi informatici e di comunicazione e delle tecnologie.

Roquette in qualità di titolare del trattamento dei dati deve conformarsi ai requisiti che regolano la protezione dei dati by design durante lo sviluppo di un software e quando commissiona sistemi, soluzioni e servizi.

Tali requisiti devono quindi essere inclusi anche nei contratti stipulati con i fornitori e quando ci si avvale di consulenti (cfr. i nostri standard con i sub-contratto).

Regola	Riferimento Q-Docs	Riferimento GDPR
• Sicurezza, privacy e protezione dei dati by design e by default	DDPG007EN Regola 3	Art. 25

Checklist:

- ☑ Rivedere la valutazione dell'impatto della protezione dei dati (DPIA)
- ☑ Evitare, limitare o ridurre al minimo la necessità di raccogliere e trattare dati personali sensibili
- ☑ Limitare e ridurre al minimo l'esposizione di funzionalità non necessarie e di dati personali nell'interfaccia utente
- ☑ Anonimizzare o pseudonimizzare i dati personali ogniqualvolta possibile
- ☑ Tutte le configurazioni rispettose della privacy devono essere by default
- ☑ Il tracciamento tra un sito web e l'altro deve essere disabilitato di default
- ☑ Revoca del consenso attraverso un menu all'interno del software. Tenete a mente che la raccolta di dati personali deve essere interrotta quando viene revocato il consenso
- ☑ Le impostazioni devono essere presentate in un menu nel quale l'interessato può consapevolmente scegliere di "modificare" le impostazioni sulla privacy a un livello più restrittivo
- ☑ Il tracciamento del dispositivo deve essere disabilitato di default

Formiamo i nostri dipendenti e miglioriamo i nostri processi interni.

- Linee guida su Community Rete protezione dati.
- Metodologie: Revisione della sicurezza e della conformità in progetti e contratti.
- Formazione sulla piattaforma HR.

Notifica di violazione dei dati

Cosa si intende per violazione dei dati personali?

Violazione dei dati personali indica una 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.

Ciò significa che una violazione è molto più di una ***perdita*** *di dati personali.*

Esempi:

- Perdita del database di un cliente
- Divulgazione della valutazione delle prestazioni dei dipendenti

Le nostre responsabilità:

Dobbiamo applicare regole idonee a trattare eventuali violazioni dei dati personali al fine di limitarne l'impatto sugli interessati e evitarne il ripetersi.

Regole	Riferimento Q-Docs	Riferimento GDPR
• Notifica di violazione dei dati personali al Data Protection Officer (Responsabile della protezione dei dati)	DDPG008EN Regola 1	Art. 33
• Notifica di violazione dei dati personali all'autorità di controllo	DDPG008EN Regola 2	
• Comunicazione di violazione dei dati personali all'interessato	DDPG008EN Regola 3	Art. 34

Chi dobbiamo contattare in caso di violazione dei dati?

Contattare il Responsabile della protezione di dati (Data Protection Officer) all'indirizzo dpo@Roquette.com e anche la linea di segnalazione confidenziale di Roquette alert@Roquette.com.

Quanto tempo abbiamo a disposizione per riferire una violazione?

Dobbiamo riferire una violazione soggetta a obbligo di notifica all'autorità di controllo senza ingiustificato ritardo, comunque non oltre 72 ore dopo esserne venuti a conoscenza.

Quali violazioni dobbiamo notificare all'Autorità di Controllo competente?

Dobbiamo notificare all'autorità di controllo competente solo una violazione che potrebbe comportare un rischio per i diritti e le libertà delle persone. Se la mancata risoluzione di tale violazione potrebbe avere un effetto negativo significativo sulle persone. Ad esempio:

- provoca discriminazione;
- danno alla reputazione;
- perdite di natura economica; o
- perdita di riservatezza o qualsiasi altro svantaggio economico o sociale significativo.

Dobbiamo valutare caso per caso e essere in grado di giustificare la decisione di notificare una violazione all'autorità di controllo.

Quando dobbiamo notificare la violazione alle persone interessate?

Se una violazione potrebbe comportare un **rischio elevato** per i diritti e le libertà delle persone, dobbiamo informare direttamente le persone interessate senza ingiustificato ritardo.
Il dovere di notificare una violazione a una persona non si applica se:

- abbiamo messo in atto le misure tecniche e organizzative appropriate che sono state applicate ai dati personali interessati dalla violazione;
- abbiamo adottato ulteriori misure per evitare il ripetersi di eventuali rischi elevati relativi ai diritti e alle libertà delle persone; o
- fossero necessari sforzi eccessivi per farlo.

Se la comunicazione di una violazione comportasse sforzi eccessivi, dobbiamo rendere disponibile l'informazione alle persone con un altro mezzo, egualmente efficace, come ad esempio una comunicazione pubblica.

Chi dobbiamo contattare in caso di violazione dei dati?

Si prega di contattare il **Responsabile della Protezione dei Dati** all'indirizzo dpo@Roquette.com e/o di segnalare l'incidente tramite il nostro modulo web "Privacy Alert".

Se avete bisogno di segnalare una potenziale violazione della conformità, potete mettervi in contatto con il vostro abituale punto di contatto o segnalare un problema tramite il dispositivo di allarme riservato Roquette: Speakup©.

Revisione e monitoraggio

Ricordiamo che:

Roquette si impegna a:

- ☑ garantire il **monitoraggio** legislativo e tecnologico dei requisiti sulla protezione dei dati,
- ☑ **revisionare** e **migliorare** il sistema di gestione della protezione dei dati (DPMS)

al fine di tenere conto delle evoluzioni normative e tecnologiche e delle limitazioni interne dei servizi. [DDPG009EN]

Le nostre responsabilità:

Regole	Riferimento Q-Docs	Riferimento GDPR
• Assicurare il monitoraggio e la revisione legislativi e tecnologici sulla protezione dei dati personali	DDPG009EN Regola 1	Buone pratiche
• Monitorare regolarmente l'implementazione del DPMS e le direttive sulla protezione dei dati	DDPG009EN Regola 2	
• Rivedere regolarmente la politica di protezione dei dati personali e la documentazione del DPMS	DDPG009EN Regola 3	

Formiamo i nostri dipendenti e miglioriamo i nostri processi interni.

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

Privacy & Data Protection News

Audit Management
Manage Internal/External Audits

Progettare e supportare il nostro programma di Privacy

Software di ricerca sulla normativa:

Utilizziamo una piattaforma che offre una suite di soluzioni in materia di privacy ideata per aiutarci a monitorare gli sviluppi normativi, mitigare il rischio e raggiungere una conformità globale:

- ☑ Tracciabilità della normativa
- ☑ Grafici comparativi transfrontalieri
- ☑ Note orientative
- ☑ Portale GDPR
- ☑ Modelli e checklists
- ☑ Chiedere a un analista
- ☑ Ricerca giuridica

Verifica e revisione del sistema di gestione della protezione dei dati:

Realizziamo delle verifiche interne per determinare se gli input dei DPMS sono:

- ☑ conformi ai requisiti di questa Guida, alla Politica e alla legislazione o ai regolamenti applicabili;
- ☑ sono attuati e conservati in maniera efficace, e
- ☑ eseguiti come previsto.

Effettuiamo una revisione del DPMS per assicurarci che rimanga adeguato e che siano individuati i miglioramenti nel processo DPMS.

Per farlo, gli input sono:

- ☑ Obiettivi, controlli, processi e procedure del DPMS;
- ☑ Risultati di verifiche e controlli della conformità precedenti;
- ☑ Feedback delle parti interessate;
- ☑ Tecniche, prodotti o procedure che potrebbero essere usati nell'organizzazione per migliorare le performance e l'efficacia del DPMS;
- ☑ Stato delle azioni preventive e correttive;
- ☑ Vulnerabilità o minacce non adeguatamente considerate nella valutazione del rischio precedente;
- ☑ Risultati delle misurazioni di efficacia;
- ☑ Azioni successive alle precedenti revisioni di gestione;
- ☑ Eventuali cambiamenti che potrebbero interessare il DPMS; e
- ☑ Raccomandazioni su possibili miglioramenti.

Documenti di riferimento

- [Codice di condotta] Codice di condotta del Gruppo Roquette
- [GDPG001EN] Glossario e definizioni relativi alla protezione dei dati
- [MDPG001EN] Manuale sulla protezione dei dati personali
- [DDPG001EN] Direttiva sulla cultura del rispetto della privacy e la protezione dei dati
- [DDPG002EN] Direttiva sulla legittimità del trattamento dei dati personali
- [DDPG003EN] Direttiva sulla valutazione dell'impatto sulla privacy
- [DDPG004EN] Direttiva sul trattamento di dati sensibili
- [DDPG005EN] Direttiva sulla registrazione delle attività di trattamento
- [DDPG006EN] Direttiva sulla conformità con i diritti delle persone
- [DDPG007EN] Direttiva sulla sicurezza dei dati personali
- [DDPG008EN] Direttiva sulla notifica di una violazione dei dati personali
- [DDPG009EN] Direttiva sulla revisione del sistema di gestione della protezione dei dati personali
- [DSUG001EN] Direttiva sulla protezione delle informazioni
- [DSUG006EN] Gestione della direttiva sulla sicurezza informatica
- [DSUG016EN] Direttiva sulla sicurezza degli appaltatori

Bibliografia

[Carta UE] Carta dei diritti fondamentali dell'Unione europea, 2010/C 83/02.

[RGPD] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 sulla protezione delle persone fisiche in materia di trattamento dei dati personali e sul libero movimento di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

[DP-Legge] Legge francese sulla protezione dei dati n°. 78-17 del 6 gennaio 1978, modificata 25.

[WP29 – Linee guida] Linee guida per l'individuazione di un'autorità di controllo principale del titolare o responsabile | WP 244 rev.01 (5 aprile 2017).

[WP29- Linee guida] Linee guida sulla valutazione dell'impatto della protezione dei dati (DPIA) e determinare quando un trattamento "potrebbe rappresentare un rischio elevato" ai fini del Regolamento 2016/679 | WP 248 rev.01 (13 ottobre 2017).

[WP29- Linee guida] Linee guida sull'applicazione e la definizione di sanzioni amministrative ai fini del Regolamento 2016/679 | WP 253 (21 ottobre 2017).

[WP29- Linee guida] Linee guida sulla decisione individuale automatizzata e la profilazione ai fini del Regolamento 2016/679 | WP 251 rev.01 (13 febbraio 2018).

[WP29 – Linee guida] Linee guida sui responsabili della protezione dei dati ('DPO') | WP 243 rev.01 (5 aprile 2017).

[WP29- Linee guida] Linee guida sulla trasparenza ai sensi del Regolamento 2016/679 | WP260 rev.01 (11 aprile 2018).

[WP29- Linee guida] Linee guida sul consenso ai sensi del Regolamento 2016/679 | WP259 rev.01 (11 aprile 2018).

[EDPB – Parere] Parere 23/2018 sulla proposta della Commissione di produzione e ordini di sequestro conservativo europei per prove elettroniche in materia penale (Art. 70.1.b) (26 settembre 2018).

[EDPB – Parere] Parere 28/2018 riguardante il progetto della Commissione europea per l'attuazione della decisione sull'appropriata protezione dei dati personali in Giappone (5 dicembre 2018).

[EDPB – Parere] Parere 14/2019 sul progetto Clausole contrattuali standard presentata da DK SA (Articolo 28(8) RGPD) (12 luglio 2019).

[EDPB- Raccomandazione] Raccomandazione 01/2019 sul progetto di elenco del Garante europeo della protezione dei dati in merito alle operazioni di trattamento soggette ai requisiti della valutazione dell'impatto della protezione dei dati (Articolo 39(4) del Regolamento (UE) 2018/1725) (10 luglio 2019).

[EDPB – EDPS Risposta congiunta] EPDB-EDPS Risposta congiunta al Comitato LIBE sull'impatto del Cloud Act americano sul quadro giuridico europeo per la protezione dei dati personali (Allegato) (10 luglio 2019).

[EDPB Parere] Parere 13/2019 sul progetto di elenco dell'autorità di controllo competente francese relativo alle operazioni di trattamento esenti dai requisiti di valutazione dell'impatto sulla protezione dei dati (Articolo 35(5) RGPD) (10 luglio 2019).

Fonti

- Commission Nationale de l'Informatique et des Libertés
  - https://www.cnil.fr/en/home
  - Settembre 2019
  - Licenza: CC-BY-ND 3.0 FR
- Information Commissioner's Office
  - https://ico.org.uk/
  - Settembre 2019
  - Autorizzato ai sensi di Licenza governativa aperta
- Unione europea
  - https://eur-lex.europa.eu
  - 1998-2019
- https://www.iso.org/home.html
- https://www.dataguidance.com/
- https://www.onetrust.com/
- https://www.corporatefiction.fr/
- https://pixabay.com/fr/service/license/

Vale come riferimento la versione inglese della presente Guida.
Le traduzioni del presente documento possono essere soggette a interpretazione.
Prima edizione: Settembre 2019
Pubblicato da ROQUETTE FRERES
Progettazione editoriale e grafica: Compliance Office
Fotografia: non coperta da diritti

ROQUETTE

Offering the best of nature™