Policy per la protezione della privacy e dei dati personali

Rif. Documento	**17-0060**
Versione:	**01-ITA**
Data:	**23 gennaio 2019**
Autore:	**Alex Kiss**
Traduzione a cura di:	**Francesca Sernissi**
Proprietario:	**Data Protection Officer**

Storia delle revisioni

Versione	Data	Autore della Revisione	Riassunto dei cambiamenti
01	30 ottobre 2018	Alex Kiss	Creato
01-ITA	23 gennaio 2019	Francesca Sernissi	Tradotto in Italiano

Distribuzione

Nome	Titolo

Approvazione

Nome	Posizione	Firma	Data

Indice dei contenuti

Elenco delle tabelle

1 Introduzione

Nelle sue operazioni quotidiane, Camlin Group fa uso di una varietà di dati riguardanti soggetti identificabili, inclusi i dati relativi a:

- Dipendenti attuali, passati e potenziali
- Clienti
- Utenti dei suoi siti Web
- Iscritti
- Altre parti interessate

Nel raccogliere e utilizzare questi dati, l'organizzazione è soggetta a una varietà di normative che verificano come tali attività possono essere eseguite e le misure di sicurezza che devono essere messe in atto per proteggerle.

Lo scopo di questa politica è di definire la legislazione pertinente e descrivere i passi che il gruppo Camlin sta adottando per assicurarsi che sia conforme ad essa.

Questo controllo si applica a tutti i sistemi, persone e processi che costituiscono i sistemi informativi dell'organizzazione, compresi i membri del consiglio di amministrazione, i dirigenti, i dipendenti, i fornitori e altre terze parti che hanno accesso ai sistemi del Camlin Group.

Le seguenti politiche e procedure sono rilevanti per questo documento:

- Processo di valutazione dell'impatto sulla protezione dei dati
- Procedura di mappatura dei dati personali
- Procedura legittima di valutazione degli interessi
- Procedura di risposta agli incidenti riguardanti la *Information Security*
- Ruoli e responsabilità legati al *General Data Protection Regulation* (GDPR)
- Policy di conservazione e protezione dei dati

2 Policy sulla privacy e sulla protezione dei dati personali

2.1 General Data Protection Regulation

Il *General Data Protection Regulation* 2016 (GDPR) è una delle normative più significative che influenzano il modo in cui Camlin Group svolge le proprie attività di elaborazione delle informazioni. Imposte significative sono applicabili se si ritiene che una violazione sia avvenuta in base al GDPR, la quale è progettata per proteggere i dati personali dei cittadini dell'Unione Europea. È politica di Camlin Group garantire che la nostra conformità al GDPR e ad altre normative pertinenti sia chiara e dimostrabile in ogni momento.

2.2 Definizioni

Ci sono in totale 26 definizioni elencate all'interno del GDPR e, pertanto, non riteniamo appropriato riprodurle tutte nel presente documento. Tuttavia, le definizioni più significative relative a questa normativa sono le seguenti:

I Dati Personali sono definiti come:

qualsiasi informazione relativa a una persona fisica identificata o identificabile ("interessato"); una persona fisica identificabile è una persona che può essere identificata, direttamente o indirettamente, in particolare facendo riferimento a un identificatore come un nome, un numero di identificazione, dati relativi all'ubicazione, un identificatore online o uno o più fattori specifici fisici, fisiologici, identità genetica, mentale, economica, culturale o sociale di quella persona fisica;

'processing' (trattamento) significa*:*

qualsiasi operazione o insieme di operazioni eseguite su dati personali o su serie di dati personali, anche con strumenti automatizzati, quali raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o alterazione, reperimento, consultazione, uso, divulgazione da parte di trasmissione, diffusione o altrimenti messa a disposizione, allineamento o combinazione, limitazione, cancellazione o distruzione;

'controller' (responsabile del trattamento) significa*:*

la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro ente che, da solo o in collaborazione con altri, determina le finalità e i mezzi del trattamento di dati personali; se le finalità e i mezzi di tale trattamento sono determinati dalla legge dell'Unione o dello Stato membro, il responsabile del trattamento o i criteri specifici per la sua nomina possono essere previsti dalla legislazione dell'Unione o dello Stato membro;

2.3 Principi relativi al trattamento di dati personali

Vi sono numerosi principi fondamentali su cui si basa il GDPR.

Tali principi sono di seguito riportati:

1. I dati personali devono essere:

a) trattati in modo lecito, equo e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");

(b) raccolti per scopi determinati, espliciti e legittimi e non ulteriormente trattati in modo incompatibile con tali scopi; l'ulteriore trattamento ai fini dell'archiviazione nell'interesse pubblico, a fini di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, non è considerato incompatibile con le finalità iniziali ("limitazione delle finalità");

(c) adeguati, pertinenti e limitati a quanto necessario in relazione agli scopi per i quali sono trattati ("minimizzazione dei dati");

(d) accurati e, ove necessario, aggiornati; deve essere adottato ogni ragionevole sforzo per garantire che i dati personali ritenuti inaccurati, tenendo conto delle finalità per cui sono trattati, siano cancellati o rettificati senza indugio ("accuratezza");

(e) conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore a quello necessario per gli scopi per i quali i dati personali sono trattati; i dati personali possono essere conservati per periodi più lunghi nella misura in cui i dati personali saranno trattati esclusivamente a fini di archiviazione nell'interesse pubblico, a fini di ricerca scientifica o storica o a fini statistici ai sensi dell'articolo 89, paragrafo 1, subordinatamente all'attuazione degli opportuni strumenti tecnici e organizzativi le misure richieste dal presente regolamento al fine di salvaguardare i diritti e le libertà dell'interessato ("limitazione dello stoccaggio");

(f) trattati in modo tale da garantire un'adeguata sicurezza dei dati personali, compresa la protezione contro il trattamento non autorizzato o illecito e contro la perdita accidentale, la distruzione o il danneggiamento, ricorrendo a misure tecniche o organizzative appropriate ("integrità e riservatezza").

2. Il controller è responsabile di quanto riportato nel paragrafo 1 ("responsabilità") e può dimostrare la conformità rispetto ad esso.

Camlin Group garantirà il rispetto di tutti questi principi, sia nel trattamento che svolge attualmente, sia come parte dell'introduzione di nuovi metodi di trattamento dei dati, quali i nuovi sistemi IT.

2.4 Diritti degli Interessati

Ai sensi del GDPR, l'interessato detiene inoltre dei diritti. Questi consistono in:

1. Il diritto di essere informato
2. Il diritto di accesso
3. Il diritto di rettifica
4. Il diritto alla cancellazione
5. Il diritto di limitare il trattamento
6. Il diritto alla portabilità dei dati
7. Il diritto di obiettare
8. Diritti in relazione al processo decisionale automatizzato e alla profilazione.

Ciascuno di questi diritti è supportato da procedure appropriate all'interno del Gruppo Camlin che consentono di intraprendere le azioni necessarie entro i termini indicati nel GDPR.

Questi termini sono mostrati nella Tabella 1.

Richiesta dell'interessato	**Termini**
Il diritto di essere informato	Quando i dati vengono raccolti (se forniti dall'interessato) o entro un mese (se non forniti dall'interessato)
Il diritto di accesso	Un mese
Il diritto di rettifica	Un mese
Il diritto alla cancellazione	Senza indebito ritardo
Il diritto di limitare il trattamento	Senza indebito ritardo
Il diritto alla portabilità dei dati	Un mese
Il diritto di obiettare	Al ricevimento di obiezioni
Diritti in relazione al processo decisionale automatizzato e alla profilazione.	Non specificato

Tabella 1 – Termini per soddisfare le richieste dell'interessato

2.5 Legittimità del trattamento

Esistono sei modi alternativi in cui la legittimità di un caso specifico di trattamento di dati personali può essere stabilita in base al GDPR. È politica del gruppo Camlin

identificare le basi appropriate per il trattamento e documentarlo, in conformità con il regolamento. Le opzioni sono descritte in breve nelle seguenti sezioni.

2.5.1 Consenso

A meno che non sia necessario per una ragione consentita nel GDPR, il Gruppo Camlin otterrà sempre il consenso esplicito da parte dell'interessato per raccogliere e trattare i suoi dati. Nel caso di bambini di età inferiore ai 16 anni (un'età inferiore può essere consentita in specifici stati membri dell'UE) sarà ottenuto il consenso dei genitori. Informazioni trasparenti sul nostro utilizzo dei dati personali saranno fornite agli interessati nel momento in cui viene ottenuto il consenso e vengono spiegati i loro diritti in relazione ai dati, come il diritto di revocare il consenso. Queste informazioni saranno fornite in forma accessibile, scritte in un linguaggio chiaro e gratuitamente.

Se i dati personali non sono ottenuti direttamente dall'interessato, tali informazioni saranno fornite all'interessato entro un ragionevole periodo dopo l'acquisizione dei dati e, in ogni caso, entro un mese.

2.5.2 Esecuzione di un contratto

Laddove i dati personali raccolti e trattati siano necessari per l'adempimento di un contratto con l'interessato, non è richiesto il consenso esplicito. Questo sarà spesso il caso in cui il contratto non può essere completato senza i dati personali in questione, ad esempio una consegna non può essere effettuata senza un indirizzo presso il quale effettuarla.

2.5.3 Obbligazioni legali

Se i dati personali sono richiesti per essere raccolti e trattati al fine di rispettare la legge, non è richiesto il consenso esplicito. Questo potrebbe essere il caso per alcuni dati relativi all'occupazione e alla tassazione, ad esempio, e per molte aree affrontate dal settore pubblico.

2.5.4 Interessi vitali dell'interessato

Nel caso in cui i dati personali siano necessari per proteggere gli interessi vitali dell'interessato o di un'altra persona fisica, questa circostanza può essere utilizzata come base legale del trattamento. Camlin Group conserverà prove ragionevoli e documentate atte a dimostrare la sussistenza del caso, ogni qual volta questa motivazione venga utilizzato come base legale per il trattamento dei dati personali. Ad esempio, tale motivazione può essere utilizzata in circostanze quali l'assistenza sociale, in particolare nel settore pubblico.

2.5.5 Attività svolta nell'interesse pubblico

Qualora Camlin Group debba svolgere un compito che ritiene sia nell'interesse pubblico o come parte di un dovere ufficiale, il consenso dell'interessato non sarà richiesto. La valutazione dell'interesse pubblico o del dovere ufficiale sarà documentata e resa disponibile come prova, laddove richiesto.

2.5.6 Interessi legittimi

Se il trattamento di dati personali specifici è nell'interesse legittimo di Camlin Group ed è ritenuto non pregiudicare i diritti e le libertà dell'interessato in modo significativo, allora questo può essere definito come il motivo legittimo per il trattamento. Anche in questa circostanza, il ragionamento alla base di questa visione sarà documentato.

2.6 Privacy by Design

Il Gruppo Camlin ha adottato il principio della *privacy by design* e assicurerà che la definizione e la pianificazione di tutti i nuovi sistemi o di sistemi significativamente modificati, che raccolgano o elaborino dati personali, saranno soggetti a debita considerazione delle questioni relative alla privacy, incluso il completamento di una o più valutazioni dell'impatto sulla protezione dei dati.

La valutazione dell'impatto sulla protezione dei dati includerà:

- Considerazione su come i dati personali saranno trattati e per quali scopi
- Valutazione del fatto che il trattamento proposto dei dati personali sia necessario e proporzionato allo scopo o ai fini
- Valutazione dei rischi per le persone nel trattamento dei dati personali
- Quali controlli sono necessari per affrontare i rischi identificati e dimostrare la conformità con la legislazione

L'uso di tecniche come la minimizzazione dei dati e la pseudonimizzazione sarà considerato laddove applicabile e appropriato.

2.7 Contratti relativi al trattamento dei dati personali

Camlin Group si assicurerà che tutti i rapporti in esso contenuti che comportano il trattamento dei dati personali siano soggetti a un contratto documentato che include le informazioni e i termini specifici richiesti dal GDPR. Per ulteriori informazioni, consultare la *GDPR Controller-Processor Agreement Policy*.

2.8 Trasferimenti internazionali di dati personali

I trasferimenti di dati personali al di fuori dell'Unione Europea saranno attentamente esaminati prima del trasferimento in corso per garantire che rientrino nei limiti imposti dal GDPR. Ciò dipende in parte dal giudizio della Commissione europea in merito all'adeguatezza delle garanzie per i dati personali applicabili nel paese ricevente e ciò potrebbe cambiare nel tempo.

I trasferimenti di dati internazionali intragruppo saranno soggetti a contratti legalmente vincolanti definiti *Binding Corporate Rules* (BCR), che prevedono diritti esecutivi per gli interessati.

2.9 Data Protection Officer

Un ruolo definito di *Data Protection Officer* (DPO) è richiesto dal GDPR se un'organizzazione è un'autorità pubblica, se esegue un monitoraggio su larga scala o se elabora in modo particolare tipi di dati particolarmente sensibili. È necessario che il responsabile della protezione dei dati disponga di un livello appropriato di conoscenza e possa essere una risorsa interna o esternalizzata a un fornitore di servizi appropriato.

Sulla base di questi criteri, Camlin Group richiede la nomina di un responsabile della protezione dei dati.

2.10 Notifica di violazione

È politica di Camlin Group essere equo e commisurato nel considerare le azioni da intraprendere per informare le parti interessate in merito a violazioni dei dati personali. In linea con il GDPR, qualora sia nota un'infrazione che potrebbe comportare un rischio per i diritti e le libertà delle persone fisiche, l'autorità di vigilanza competente verrà informata entro 72 ore. Questa notifica sarà gestita in conformità con la nostra procedura di risposta agli incidenti di *information security*, che definisce il processo generale di gestione degli incidenti di sicurezza delle informazioni.

Ai sensi del GDPR, la DPA competente ha l'autorità di imporre una serie di multe fino al quattro percento del fatturato globale annuo o di venti milioni di euro, a seconda di quale sia il più alto, per le violazioni dei regolamenti.

2.11 Gestione della compliance con il GDPR

Le seguenti azioni sono intraprese per garantire che il Gruppo Camlin rispetti in ogni momento il principio di responsabilità sancito dal GDPR:

- La base legale per il trattamento dei dati personali è chiara e inequivocabile
- Viene nominato un responsabile della protezione dei dati con specifica responsabilità per la protezione dei dati nell'organizzazione (se necessario)
- Tutto il personale coinvolto nella gestione dei dati personali comprende le proprie responsabilità nel seguire le buone pratiche di protezione dei dati
- La formazione sulla protezione dei dati è stata fornita a tutto il personale
- Le regole riguardanti il consenso sono seguite

- Indicazioni sono disponibili per gli interessati che desiderino esercitare i loro diritti in materia di dati personali e tali richieste sono gestite in modo efficace
- Vengono effettuate revisioni periodiche delle procedure relative ai dati personali
- La privacy by design è adottata per tutti i sistemi e processi nuovi o modificati
- La seguente documentazione delle attività di elaborazione è registrata:
    - Nome dell'organizzazione e dettagli pertinenti
    - Finalità del trattamento dei dati personali
    - Categorie di persone e dati personali trattati
    - Categorie di destinatari di dati personali
    - Accordi e meccanismi per il trasferimento di dati personali verso paesi non UE, compresi i dettagli dei controlli in atto
    - Programmi di conservazione dei dati personali
    - Controlli tecnici e organizzativi rilevanti in essere

Queste azioni sono riviste periodicamente nell'ambito del processo di gestione relativo alla protezione dei dati.