creditsafe

Istruzioni per i clienti sulla GDPR

L'uso del GDPR da parte di Creditsafe per migliorare la propria attività

Introduzione

Cos'è il GDPR?

Il GDPR (Regolamento generale sulla protezione dei dati) fornirà un insieme di regole forti per la raccolta, la conservazione e il trattamento delle informazioni personali ed entrerà in vigore il 25 maggio 2018. Il GDPR è un regolamento e non una direttiva, pertanto una singola legislazione che si applica a tutti gli stati membri dell'UE.

Perché il GDPR?

Le aziende raccolgono grandi quantità di dati personali sui consumatori, dall'analisi del loro comportamento alle loro caratteristiche, quindi il tema della riservatezza e della protezione dei dati personali desta sempre maggiori preoccupazioni. Molte aziende hanno sviluppato importanti modelli aziendali basati sulla concessione di servizi in cambio della condivisione di informazioni.

Pur avendo offerto enormi opportunità, gli individui hanno sempre meno controllo sull'uso dei propri dati e sui metodi di conservazione e potrebbero pertanto essere esposti a furto, frode o altri usi impropri. Inasprendo le misure protettive, l'UE intende promuovere la fiducia e in generale ridurre il rischio per gli individui.

Il GDPR viene introdotto per riflettere il progresso della tecnologia e dei dati negli ultimi tempi. Il GDPR ha l'obiettivo di armonizzare le leggi in materia di protezione dei dati in Europa, creando un contesto comune ma soprattutto semplificando la comprensione da parte delle imprese e la gestione diretta della conformità.

A chi si applica il GDPR?

Tutte le organizzazioni che possiedono dati personali dei cittadini dell'UE saranno interessate dal GDPR. Non importa la posizione dei dati nel mondo.

Il GDPR amplia la definizione di dati personali per abbracciare qualsiasi elemento che potrebbe essere utilizzato per identificare una persona fisica, direttamente o indirettamente. Questo copre un ampio spettro di dati, partendo da nomi, fotografie, indirizzi e-mail, dati bancari e pubblicazioni sulle reti sociali, fino alle informazioni sanitarie o agli indirizzi IP, ad esempio. Il nuovo regolamento intende proteggere tali dati, sia quando sono inviati automaticamente che manualmente, su supporto cartaceo o elettronico.

Quando consideriamo le comunicazioni B2B, ovvero tra imprese, e B2C, ovvero tra impresa e consumatore, e l'ambito di applicazione del GDPR, la separazione tra i dati personali e i dati aziendali non è ben definita. Ad esempio i dati degli individui di aziende non registrate, quali lavoratori in proprio o ditte individuali, oppure i dati del direttore di un'azienda registrata, devono essere considerati dati personali identificabili secondo la definizione fornita dal GDPR.

creditsafe

Chi sono gli attori principali nel GDPR?

Le organizzazioni saranno responsabili di fronte alle autorità garanti per la protezione dei dati. La responsabilità non è un requisito nuovo, tuttavia il GDPR chiede a tutte le organizzazioni di registrare e documentare la conformità a tutti gli aspetti del GDPR applicabili. Il regolamento introduce per gli individui ulteriori diritti sui dati, inclusi maggior controllo e visibilità sull'uso dei dati personali e il diritto a richiedere la rimozione di tali informazioni o il trasferimento su richiesta.

Soggetto interessato

I soggetti interessati sono le persone fisiche (cittadini dell'UE) i cui dati vengono raccolti e trattati, ad esempio direttori, soci e titolari di un'impresa. Il GDPR prevede ulteriori diritti per i soggetti interessati con riferimento ai dati trattati e controllati dalle imprese. Questo aspetto viene normalmente definito conferimento del potere all'interessato.

Titolare del trattamento

Il titolare del trattamento determina gli scopi e i mezzi per il trattamento dei dati. Deve verificare il modo in cui vengono trattati i dati personali, dovendo rispondere delle ragioni e delle modalità per il trattamento. Gli obblighi del titolare non sono sollevati dall'esistenza del responsabile del trattamento, il GDPR prevede ulteriori obblighi per garantire che i contratti con i responsabili del trattamento siano conformi al GDPR. Creditsafe è un titolare del trattamento.

Responsabile del trattamento

Il responsabile del trattamento opera il trattamento dei dati personali per conto del titolare del trattamento. Il GDPR prevede obblighi specifici per il responsabili del trattamento; ad esempio, devono mantenere la documentazione relativa ai dati personali e alle attività di trattamento. I responsabili del trattamento hanno responsabilità giuridica quando si rendono responsabili di una violazione.

Autorità garante per la protezione dei dati

Le Autorità garanti sono autorità pubbliche che hanno il potere di vigilare sull'applicazione della legge in materia di protezione dei dati, svolgendo indagini e individuando misure correttive. Forniscono consulenze in materia di protezione dei dati e gestiscono i reclami per le violazioni del Regolamento generale sulla protezione dei dati e relative leggi nazionali. Ogni paese membro ha una autorità garante.

Responsabile della protezione dei dati

Il ruolo principale del Responsabile della protezione dei dati (RPD) è garantire che l'organizzazione tratti i dati personali dei dipendenti, clienti, fornitori o altri individui, come previsto dalle vigenti leggi in materia di protezione dei dati. Il Regolamento applicabile sulla protezione dei dati (Regolamento (CE) 45/2001) prevede la nomina di un RPD nelle istituzioni e organizzazioni dell'UE. Creditsafe ha nominato un RPD a livello del Gruppo, supportato da ruoli a livello locale ove previsto dal regolamento o dalla prassi di settore.

creditsafe

Le aree chiave del GDPR

1. **Responsabilità**

I titolari del trattamento dei dati devono essere in grado di dimostrare la conformità dell'organizzazione al GDPR. Tuttavia, la responsabilità sia del titolare che del responsabile del trattamento garantisce l'aderenza alle procedure corrette.

2. **Trasparenza**

Le organizzazioni dovranno chiarire in modo aperto e trasparente le ragioni e gli scopi della raccolta e dell'uso dei dati personali. Ovvero devono spiegare al soggetto interessato come intendono utilizzare i dati e ottenere il consenso del soggetto.

3. **Trattamento dei dati personali**

I dati personali possono essere raccolti solo per scopi specifici, espliciti e legittimi e non devono essere usati in nessun altro modo che non soddisfi tali requisiti. Di conseguenza, i dati raccolti in modo legittimo per uno scopo specifico non possono essere utilizzati per altri scopi, se non con il consenso dell'interessato o sulla base di un legittimo interesse.

4. **Diritto di accesso**

I soggetti interessati hanno il diritto di accedere ai propri dati entro 30 giorni dalla richiesta. Le organizzazioni hanno la responsabilità di garantire la cancellazione o l'aggiornamento dei dati scorretti, permettendo ai soggetti interessati di esercitare i diritti di verifica e rettifica delle informazioni personali.

5. **Diritto all'oblio**

I soggetti interessati hanno anche il diritto di richiedere la rimozione dei propri dati personali in assenza di una base legittima per la conservazione.

6. **Protezione dei dati preimpostata (Valutazione dell'impatto sulla privacy)**

Il GDPR prevede la valutazione dei tempi di conservazione dei dati personali. In circostanze con rischio elevato, sarà necessario svolgere una Valutazione dell'impatto sulla privacy. Prevede anche che la raccolta di dati personali da parte delle organizzazioni si limiti ai dati necessari per gli scopi previsti, senza eccedere nella raccolta.

7. **Sanzioni per impatto sulla privacy o per violazione dei diritti**

Per le violazioni del GDPR sono previste sanzioni fino al 4% del fatturato annuale o 20 milioni di euro, il maggiore tra i due.

8. **Riportare le violazioni**

In caso di violazione dei dati che potrebbe danneggiare o avere impatti sul soggetto interessato, il titolare del trattamento dovrà informare l'autorità garante entro 72 ore dal rilevamento di una violazione importante dei dati.

Il GDPR e Creditsafe

Creditsafe, nello svolgimento delle proprie attività, raccoglie dati relativi alle aziende e al comportamento delle stesse nel tempo, per valutarne l'affidabilità creditizia. Creditsafe fornisce ai propri clienti dati per prendere decisioni finanziarie e per la gestione del rischio durante le proprie attività. Le Informazioni personali identificabili (PII) trattate da Creditsafe sono soltanto relative ai soggetti direttamente connessi ad una società.

Creditsafe opera in un ambiente B2B (ovvero tra aziende) e possiede solo PII di individui in quanto parte di un'organizzazione, ad esempio un direttore, o in quanto l'individuo costituisce l'impresa, ad esempio un lavoratore in proprio. Creditsafe valuta esclusivamente la capacità di un'impresa di condurre o continuare a condurre affari e ad adempiere ai propri impegni contrattuali in base alle prestazioni attuali e storiche. Pertanto la tipologia e la qualità dei dati forniti ai clienti non cambierà con l'introduzione del GDPR.

Qualora i dati raccolti da Creditsafe siano considerati non adatti all'uso o non siano supportati da adeguato consenso, verranno cancellati.

Interesse legittimo nella fornitura di servizi informativi

L'Articolo 6:F del GDPR autorizza il trattamento per gli scopi connessi ai legittimi interessi del titolare del trattamento o di terzi. Consente inoltre il trattamento dei dati personali da parte dei titolari del trattamento con una ragione legittima. Questo può includere i vantaggi commerciali, ad eccezione di quando tali interessi sono superati dagli interessi o dai diritti e dalle libertà fondamentali del soggetto interessato, che richiedono la protezione dei dati personali.

Il legittimo interesse di Creditsafe è il fatto che aiutiamo i nostri clienti a prendere decisioni finanziarie basate sul rischio, al fine di permettere agli stessi di prendere decisioni aziendali e commerciali migliori. Pertanto abbiamo un legittimo interesse nell'informare le aziende di tale capacità.

Relazione titolare-titolare

Creditsafe offre una vasta gamma di prodotti ai propri clienti. Creditsafe usa la propria banca dati per fornire i servizi e può decidere per quali altri ragioni utilizzare i dati. Creditsafe agirà come titolare del trattamento, tale posizione sarà coperta dai termini e condizioni standard.

Creditsafe agisce come titolare del trattamento ogni volta che fornisce servizi al cliente: Creditsafe usa i propri dati e può decidere cosa fare con essi; potrà scegliere come utilizzarli e decidere il modo in cui svolgere un compito, quali dati includere e cosa inserire nella relazione da compilare. Questo implica la completa responsabilità di Creditsafe in tutte le attività di trattamento e deve garantire di condividere i dati personali solo quando tale condivisione è legittima.

Tutti i dati forniti da Creditsafe con i propri prodotti e servizi costituiranno una relazione da titolare a titolare con i nostri clienti per cui *non sono necessarie clausole di trattamento*. Nonostante tale relazione "da titolare a titolare" con i clienti, Creditsafe ha inserito nei propri termini e condizioni standard le clausole per la protezione dei dati.

In qualità di titolare del trattamento Creditsafe deve garantire la condivisione dei dati solo quando è legittima, pertanto Creditsafe ha previsto nei termini e condizioni il quadro per la condivisione dei dati personali e un avviso per il cliente che lo informa dell'esigenza di una propria base giuridica per usare i nostri servizi. Nei termini e condizioni di Creditsafe è incluso un elenco delle ragioni per cui un cliente può usare i nostri prodotti.

Alcuni servizi informatici specifici sono:

Inserimento ricerche

La visione non vincolante dell'autorità garante è che i termini di ricerca siano irrilevanti - l'azienda che possiede la banca dati è il titolare del trattamento per la banca dati e quando invia informazioni al cliente tramite un rapporto, il cliente diventerà titolare del trattamento per tale rapporto. Pertanto la questione principale è se le informazioni possono in primo luogo essere condivise.

Pulizia/integrazione dei dati e dati di pagamento

Creditsafe "controlla" le correzioni apportate a tali dati e quali informazioni/dati aggiuntivi devono essere inseriti come parte del servizio. Creditsafe ha la flessibilità di decidere come svolgere il compito, essendo un "titolare del trattamento" di tali dati.

I nostri clienti possono usare le nostre informazioni?

Si, tutti i nostri dati e prodotti sono allineati ai requisiti e usiamo i dati sulla base del consenso fornito o del nostro legittimo interesse.

Il Cliente sarà tenuto a stabilire le proprie basi giuridiche per il trattamento dei dati ottenuti utilizzando i servizi informatici di Creditsafe e dovrà mantenere la conformità alle Leggi in materia di protezione dei dati in relazione a tali dati. Il Cliente deve prendere atto del fatto che l'accesso ai dati personali utilizzando i servizi informatici di Creditsafe sia consentito esclusivamente quando per il Cliente esiste una base giuridica per agire in tal senso.

Questo ad esempio significa che il cliente potrà esclusivamente utilizzare i servizi informatici di Creditsafe agli scopi di verifica del credito, ricerca nuovi clienti, marketing diretto, controlli sui propri clienti, conformità, verifica e miglioramento dei dati, altri scopi aziendali legittimi di due diligence o altri scopi per le relazioni tra imprese con legittimo interesse ai sensi del GDPR.

L'allineamento di Creditsafe al GDPR

Creditsafe ha previsto un approccio aziendale totale al GDPR, rivedendo l'intera attività e i processi relativi ai dati per verificare che siano allineati ai legittimi interessi dell'azienda e per supportare i clienti nelle decisioni finanziarie grazie a valutazioni del rischio basate sui fatti. Questo processo ci permette di esaminare le fonti e usare tutti i nostri dati al fine di verificare che i nostri clienti ricevano il servizio desiderato, garantendo allo stesso tempo che nessuna delle nostre pratiche possa causare danno o pregiudizio agli individui identificati nei nostri insiemi di dati.

Comprendere le nostre fonti e la conservazione dei dati (mappatura dei dati)

In tutte le fasi di custodia dei dati dobbiamo definire cosa stiamo facendo con i dati, come vengono protetti e come possiamo garantire di non violare i diritti del soggetto interessato. Questo implica che i dati personali siano ottenuti solo per scopi specifici e legittimi, e non saranno ulteriormente trattati in modo incompatibile con tale scopo o scopi.

Comprendere come utilizziamo i dati

Quando i dati sono raccolti sulla base del legittimo interesse, per documentare il trattamento o con il consenso, Creditsafe garantirà che i dati siano adeguati, rilevanti e non eccessivi in relazione allo scopo. Creditsafe valuta in modo sistematico i propri dati per verificare il legittimo interesse.

Protezione dei diritti dell'individuo

Creditsafe ha previsto dei processi per la gestione di tutti i diritti degli individui, incluse le Richieste di accesso del soggetto interessato, il diritto all'oblio, alla correzione dei dati, alla modifica del consenso fornito e trasferimento dei dati ad un'altra piattaforma per l'uso individuale.

Integrità e trasparenza

I processi per la protezione dei dati di Creditsafe gestiscono e affrancano i dati, garantendo la piena tracciabilità di tutti i dati Creditsafe. Mostrando chiaramente la provenienza dei dati e le modifiche apportate unitamente alle ragioni di tali modifiche.

Implementazione delle misure tecniche ed organizzative adeguate

Per la protezione da trattamento illecito o non autorizzato dei dati personali e da perdita o distruzione accidentale, o danno ai dati personali, Creditsafe implementa tecnologie che permettono innanzitutto di identificare e quindi di etichettare le Informazioni personali identificabili (PII) sensibili, fornendo una protezione generale dei dati. Questo garantisce che i dati non vengano utilizzati impropriamente o rimossi dalla rete Creditsafe con azioni non autorizzate.

Di seguito sono elencate alcune delle misure adottate per proteggere i nostri sistemi e dati:

Firewall - Tutti i punti di accesso/uscita alle/dalle reti sono protetti da firewall.

- DMZs – Server accessibili al pubblico ben definiti, con segmentazione di rete interna per l'ulteriore isolamento delle risorse sensibili.
- HIDS/NIDS – Abilitati nei punti di strozzamento chiave sulla rete.
- SIEM – Monitoraggio delle reti con SIEM, con analisi e registrazione degli eventi per la sicurezza, avvisi automatici e allarmi attivi.
- Antivirus – Tutti i punti vulnerabili coperti da software antivirus, con aggiornamenti automatici tramite server di aggiornamento e internet.
- Scansione Rete/host - Scansione periodica per configurazioni vulnerabili.
- Prove di penetrazione periodiche, prove delle applicazioni web e scansione di vulnerabilità - Programma di gestione delle minacce e delle vulnerabilità adottato per la gestione dei risultati.
- Prevenzione delle perdite di dati: Creditsafe ha implementato dei controlli per proteggere i dati da perdita dovuta ad azioni non autorizzate sia sulle reti che tramite mezzi esterni.

Implementazione degli adeguati controlli

Creditsafe si impegna ad evitare i trasferimenti di dati ai territori che non rientrano nello Spazio Economico Europeo se tale territori non garantiscono un livello adeguato di protezione dei diritti e delle libertà dei soggetti interessati in relazione al trattamento dei dati personali.

Pronti a rispondere

Creditsafe ha implementato dei processi che permetteranno di rispondere in modo rapido ed efficace agli eventuali sospetti di incidente, incluse le violazioni che potrebbero avere un impatto sulle PII. Creditsafe ha previsto comunicazioni chiare e concise per i propri clienti, soggetti interessati e autorità garanti in caso di incidenti che possono avere un impatto su qualsiasi individuo.

Privacy fin dalla progettazione.

Creditsafe è consapevole del fatto che il GDPR non sia un evento fine a se stesso, piuttosto è una guida per i nostri modelli aziendali futuri in cui la privacy fin dalla progettazione è adottata nelle nostre interazioni con gli individui. Viene anche utilizzata nella nostra strategia aziendale, garantendo che tutti gli sviluppi e le decisioni aziendali future prendano in considerazione l'impatto sull'individuo prima di procedere.

Domande frequenti

Creditsafe è completamente conforme al GDPR?

Creditsafe è impegnata in un programma sul GDPR a 360 gradi per garantire che le nostre operazioni e i servizi offerti aderiscano completamente al regolamento.

Creditsafe, nello svolgimento delle proprie attività, raccoglie dati relativi ad aziende e al comportamento delle stesse nel tempo per fare valutazioni e fornire ai propri clienti dati per prendere deisioni finanziarie e gestire il rischio. Le PII trattate da Creditsafe sono soltanto relative ai soggetti direttamente connessi ad una società.

Creditsafe opera in un ambiente B2B, ovvero tra imprese. Possediamo solo PII di individui in quanto parte di un'organizzazione, ad esempio un direttore, o in quanto l'individuo costituisce l'impresa, ad esempio un lavoratore in proprio. Valutiamo esclusivamente la capacità di un'impresa di condurre o continuare a condurre affari e ad adempiere ai propri impegni contrattuali in base alle prestazioni storiche. Pertanto la tipologia e la qualità dei dati forniti ai clienti non cambierà con l'introduzione del GDPR. Qualora i dati raccolti da Creditsafe siano considerati non adatti all'uso o non siano supportati da adeguato consenso, verranno cancellati.

Quali software e codifiche di sicurezza sono previste per proteggere tutti i dati raccolti e/o trattati da Creditsafe?

- Creditsafe possiede la certificazione ISO27001, regolata dalla FCA ed è un titolare del trattamento dei dati registrato presso l' Information Commissioner's office del Regno Unito.
- Creditsafe opera attraverso un centro dati Tier3+ UK, con certificazione ISO9001, ISO14001, ISO27001, ISAE3402, SSAE16 e conforme agli standard di sicurezza dei dati per il settore delle carte di pagamento.
- Sicurezza fisica completa del centro dati, incluso progetto di parete a 6 strati, vigilanza 24/7, recinzione anti intrusione, sistema anti intrusione a filo digitale, telecamere a circuito chiuso e costruzione conforme agli standard antisismici della California.

I controlli di sicurezza di Creditsafe includono:

- Firewall - Tutti i punti di accesso/uscita alle/dalle reti sono protetti da firewall.
- DMZs – Server accessibili al pubblico ben definiti, con segmentazione di rete interna per l'ulteriore isolamento delle risorse sensibili.
- HIDS/NIDS – Abilitati nei punti di strozzamento chiave sulla rete.
- SIEM – Monitoraggio delle reti con SIEM, con analisi e registrazione degli eventi per la sicurezza, avvisi automatici e allarmi attivi.
- Antivirus – Tutti i punti vulnerabili coperti da software antivirus, con aggiornamenti automatici tramite server di aggiornamento e internet.
- Codifica dei dati.
- Scansione Rete/host - Scansione periodica per configurazioni vulnerabili.
- Prove di penetrazione periodiche, prove delle applicazioni web e scansione di vulnerabilità - Programma di gestione delle minacce e delle vulnerabilità adottato per la gestione dei risultati.
- Backup- I dati vengono replicati ad intervalli di 5 minuti dall'ambiente di produzione di Creditsafe ad un ambiente aziendale dedicato per la continuità. La piattaforma viene dimensionata e configurata per usare un'elevata disponibilità, permettendo failover automatici del server.

Dati commerciali di Creditsafe

Come vengono preparati i dati commerciali da Creditsafe per il GDPR?

Creditsafe ha predisposto un programma completo per il GDPR per garantire che tutti i dati siano raccolti e utilizzati in modo lecito, con il consenso o per legittimo interesse. L'uso dei dati viene mappato in ogni momento ed è soggetto a valutazioni rigorose del rischio e dell'impatto sulla riservatezza dei dati.

Quale consenso richiede Creditsafe alle aziende che forniscono le proprie informazioni?

Il Consenso fornito a Creditsafe dipende dalla destinazione d'uso dei dati raccolti in un momento specifico, ad es. consenso all'uso, per la ricezione di informazioni commerciali, per la ricezione di telefonate e per l'aggiornamento dei dati a registro per futuri contatti.

Nei casi in cui non sia disponibile il consenso, l'Articolo 6 del GDPR autorizza il trattamento per gli scopi connessi ai legittimi interessi del titolare del trattamento o di terzi. Il legittimo interesse di Creditsafe è il fatto che aiutiamo i nostri clienti a prendere decisioni finanziarie basate sul rischio, al fine di permettere agli stessi di prendere decisioni aziendali e commerciali migliori. Pertanto abbiamo un legittimo interesse nell'informare le aziende di tale capacità anche quando cercano di sviluppare la propria attività.

Dove vengono conservati i dati, nel Regno Unito?

Tutti i dati di Creditsafe sono conservati nel Regno Unito o nel SEE su server sicuri completamente coperti per il ripristino in seguito a disastro.