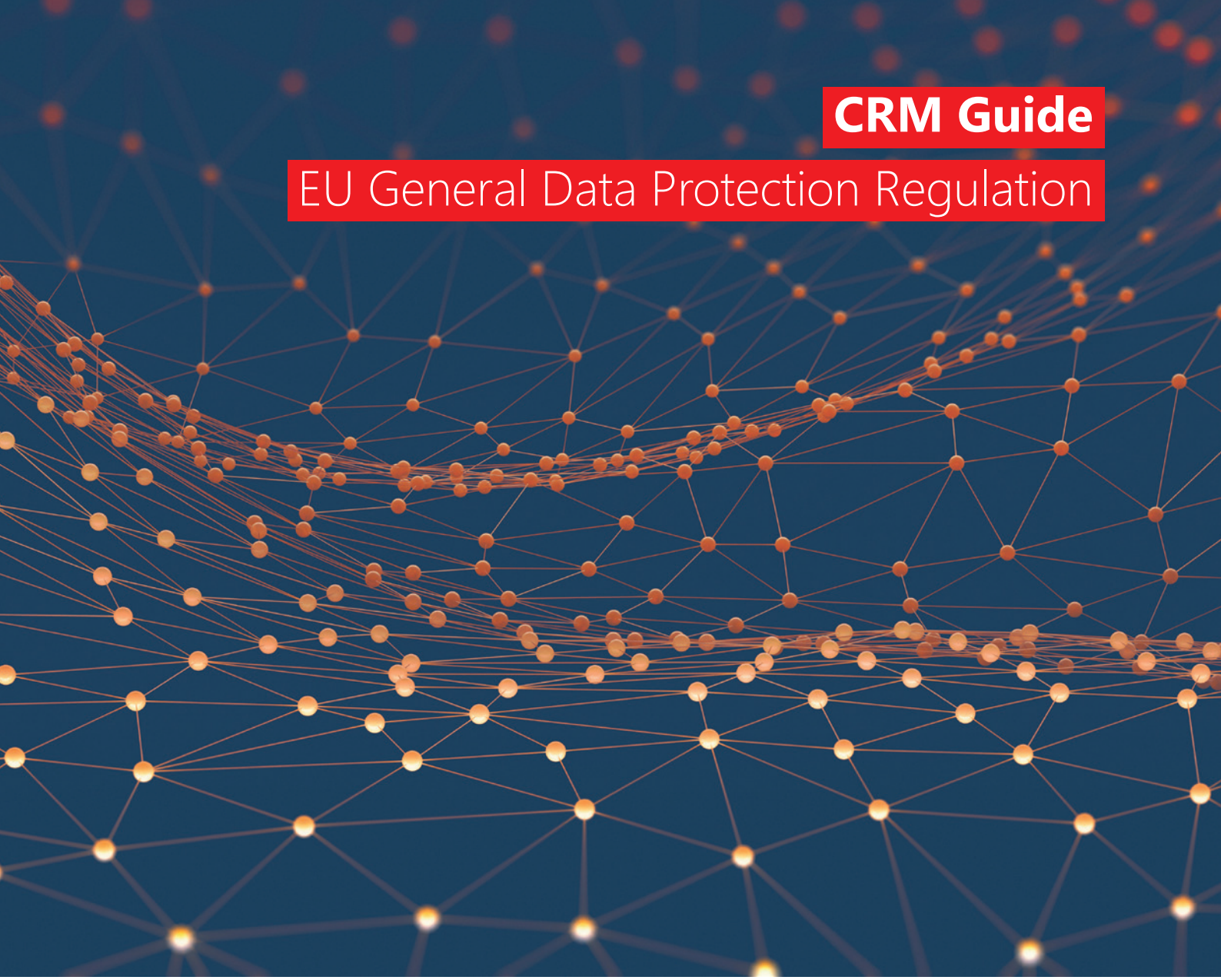
CRM Guide

EU General Data Protection Regulation



Come il CRM può supportare nel tuo viaggio verso il GDPR

CAS SOFTWARE

CAS-Weg 1 - 5, 76131 Karlsruhe, Germany, www.cas-crm.com

April 2018

Contenuti

Introduzione

Benvenuti nel mondo digitale di oggi. Con tutti i suoi dati, informazioni e reti, Internet offre fantastiche possibilità e possibilità. E ovviamente ci aspettiamo di raccogliere e condividere informazioni e conoscenze, comunicare in tutto il mondo, essere accessibili 24 ore su 24, 7 giorni su 7 e avere accesso a tutti i tipi di dati, indipendentemente dalla posizione. Con la semplice pressione di un pulsante possiamo effettuare ordini e pagare beni e servizi, nonché concludere transazioni online, alcune delle quali hanno ramificazioni di ampia portata. Molti dei processi vengono eseguiti automaticamente come per magia.

Tuttavia, anche la facilità d'uso ha i suoi rischi: furto e uso improprio dei dati, sorveglianza, "essere umano trasparente" e manipolazione sono solo alcuni di questi. Le normative sulla protezione dei dati dell'Unione Europea ci proteggono dai rischi connessi alle nostre transazioni quotidiane di dati, indipendentemente dal fatto che agiamo come persona privata, consumatore o cliente.

Il GDPR si applicherà dal 25 maggio 2018 ed è stato concepito per aumentare la trasparenza e migliorare la protezione dei dati personali.

Finora sono state soprattutto le multe elevate fino a 20 milioni di euro e le tante domande senza risposta che hanno dominato i titoli dei giornali.
Per le aziende, tuttavia, il GDPR rappresenta anche un'ottima opportunità per stabilire buone relazioni con i clienti basate sulla fiducia e per svilupparle con attività di marketing, vendita e assistenza mirate e orientate alle esigenze dei clienti.

In questa guida spieghiamo in termini generali le problematiche coperte dal GDPR e l'impatto sulla gestione dei clienti nelle aziende. Troverai anche una serie di suggerimenti e trucchi molto utili su come rispettare le normative legali. Tieni presente che questi suggerimenti possono essere formulati solo in termini molto generali. E ti preghiamo di tenere presente che ci sono ulteriori leggi e regolamenti nazionali che devono essere presi in considerazione in materia di privacy e sicurezza dei dati. Se hai domande specifiche, ti consigliamo di consultare il tuo responsabile della protezione dei dati o un avvocato specializzato in questo campo.

Preparati per il GDPR. Saremo lieti di supportarti con le nostre soluzioni CRM e il nostro know-how!

Tuo
CAS Software AG
www.cas-crm.com

in collaborazione con

Thomas Heimhalt
DATENSCHUTZ *perfect* GbR
Consulente Data protection, responsabile e revisore
(TÜV – Technical Certification Body)

GDPR

La dignità umana è inviolabile. La tutela delle persone fisiche rispetto al trattamento dei dati personali è un diritto fondamentale: ogni persona ha diritto alla protezione dei dati personali che lo riguardano.[1]

Al fine di tutelare questi diritti fondamentali e in vista di un'armonizzazione a livello europeo, è stato redatto il nuovo Regolamento generale UE sulla protezione dei dati, GDPR. È applicabile dal **25 maggio 2018**.

Il nuovo regolamento offre ai cittadini dell'UE e del SEE un maggiore controllo sui propri dati personali e garantisce che i dati personali siano protetti in tutta Europa. Pertanto, ci sarà meno possibilità di registrare e utilizzare i dati personali per scopi commerciali. Sebbene non sia l'obiettivo del regolamento impedire o complicare le transazioni commerciali. Al contrario, l'obiettivo è rendere più trasparenti la conservazione e l'utilizzo dei dati personali.

Il GDPR si applica a tutte le aziende che vendono prodotti a cittadini europei e che conservano o elaborano i loro dati personali, indipendentemente dall'ubicazione della propria sede principale ("principio della localizzazione del mercato").

Potrebbero essere state mantenute ulteriori normative precedentemente applicate in ciascuno stato membro dell'UE, ma i loro termini devono essere conformi al GDPR.

Il nostro esperto consiglia

Prendi sul serio il GDPR e non perdere tempo ad adottare le misure necessarie per il rispetto delle disposizioni, poiché le **sanzioni sono state notevolmente aumentate**: le aziende che violano la protezione dei dati rischiano sanzioni sostanziali fino a 20 milioni di euro o fino al quattro per cento del le vendite globali dell'anno precedente dell'intero gruppo, a seconda di quale sia la somma più alta. Inoltre, gli interessati che hanno subito danni materiali o immateriali hanno diritto al risarcimento dei danni.

[1] Ai sensi dell'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea (la "Carta") e dell'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea (TFUE)

Panoramica delle disposizioni più importanti del GDPR

Il GDPR

- stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati e
- protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il loro diritto alla protezione dei dati personali, per cui
- la libera circolazione dei dati personali nell'UE non è né limitata né vietata per motivi connessi alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Cosa sono i dati personali?

Ai fini del GDPR, per dato personale si intende qualsiasi informazione relativa a una persona fisica identificata o identificabile ("interessato"), come un nome, un numero di identificazione, dati relativi all'ubicazione, un identificatore online o a uno o più fattori specifici all'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica – senza distinguere tra dati personali nell'ambiente privato, pubblico o lavorativo di una persona, poiché i rapporti commerciali sono sempre mantenuti da singole persone (fisiche).[2]

Consiglio pratico per l'utente

Nell'ambito dell'assistenza clienti e delle relazioni con i clienti, è spesso normale per noi divulgare informazioni private come date di nascita, stato di famiglia e hobby. Prima di archiviare tali dati nel CRM, è necessario verificare se queste informazioni debbano essere effettivamente archiviate o elaborate, idealmente solo se sono rilevanti per il contratto o se il cliente ha dato il suo permesso.

[2] Art. 4 GDPR

Quali processi sono coperti?

In generale, la protezione dei dati comprende tutti i processi che coinvolgono dati personali. Il regolamento nel frattempo riassume questo sotto il termine "trattamento".

Quindi "elaborazione" è inteso come significato[3]:

- qualsiasi operazione o insieme di operazioni compiute su dati personali o su insiemi di dati personali,
- anche con mezzi automatizzati
- ad esempio
  - la collezione,
  - la registrazione,
  - l'organizzazione,
  - la strutturazione,
  - il deposito,
  - l'adattamento o la modifica,
  - il recupero,
  - la consultazione,
  - l'utilizzo,
  - la comunicazione per trasmissione, diffusione o altro
  - l'allineamento o la combinazione,il vincolo,
  - la cancellazione o
  - la distruzione

[3] Art. 4 GDPR

Principi

Il GDPR continua a prescrivere precedenti principi di protezione dei dati[4] e a svilupparli ulteriormente

Legittimità, correttezza e trasparenza

I dati personali saranno trattati in modo lecito, con correttezza e con trasparenza nei confronti dell'interessato.

Limitazione dello scopo

I dati personali saranno raccolti per finalità determinate, esplicite e legittime e ulteriormente trattati in modo non incompatibile con tali finalità. Qualora la finalità originaria dovesse cambiare, questa dovrà essere comunicata.

Minimizzazione dei dati

Less is more: i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali sono trattati.

Precisione

I dati personali devono essere esatti e, ove necessario, aggiornati. Occorre adottare ogni ragionevole misura per garantire che i dati personali inesatti, rispetto alle finalità per le quali sono trattati, siano cancellati o rettificati senza indugio.

Limitazione di archiviazione

I dati personali sono conservati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario alle finalità per le quali sono trattati. Successivamente, i dati personali devono essere cancellati o resi anonimi. A tal proposito, vanno tenute in considerazione le eccezioni previste dal GDPR.

Integrità e riservatezza

I dati personali sono trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione contro il trattamento non autorizzato o illecito e contro la perdita, la distruzione o il danneggiamento accidentali, utilizzando misure tecniche o organizzative adeguate.

Conformità e responsabilità

Il responsabile del trattamento è responsabile e deve essere in grado di dimostrare il rispetto Art. 5 (1) GDPR.

[4]Art. 5 GDPR

Lawfulness of processing

Il principio generale per il trattamento dei dati personali è il cosiddetto diritto di autorizzazione.[5] In base a ciò, il trattamento dei dati personali è ammissibile solo se il cliente interessato ha prestato il consenso al trattamento (o si applica una valida eccezione ai sensi dell'Art. 6 GDPR).

Condizioni di consenso

Questo consenso è soggetto a determinate condizioni[6], inter alia:

Onere della prova

Il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha acconsentito al trattamento dei propri dati personali per una o più finalità specificate.

Chiaro e distinguibile

Se il consenso scritto è prestato in relazione ad altre materie, la richiesta di consenso al trattamento dei suoi dati deve essere formulata in modo tale da essere chiaramente distinguibile dalle altre materie. Inoltre, la richiesta deve essere formulata in forma comprensibile e facilmente accessibile, utilizzando un linguaggio chiaro e semplice.

Diritto di revocare il consenso

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. Prima di prestare il consenso, l'interessato ne è informato. Il ritiro deve essere facile quanto il consenso.

Volontario

Il consenso è valido solo se l'interessato lo ha fornito di propria spontanea volontà. Le circostanze del problema devono essere prese in considerazione per determinare se il consenso è stato dato volontariamente.

Riferimento a finalità e trattamento

È necessario informare l'interessato dello scopo previsto del trattamento. In alcuni singoli casi, l'interessato può negare il consenso o chiedere di conoscere la finalità del trattamento, nel qual caso è necessario informarlo anche delle conseguenze dell'opt-out.

[5] Art. 6 GDPR
[6] Art. 7 GDPR. Per quanto riguarda il consenso di un minore in relazione ai servizi della società dell'informazione, devono essere prese in considerazione ulteriori condizioni. Il limite di età di 16 anni deve essere rispettato.

Diritti dell'interessato

Con il GDPR, le singole persone ottengono un maggiore controllo sui propri dati (diritti dell'interessato[7]) – questi includono, tra l'altro:

Diritto alla trasparenza e all'informazione

L'interessato deve essere informato prima della raccolta e della registrazione dei suoi dati personali. Lui o lei acconsente espressamente alla registrazione di questi dati.

Diritto di accesso

L'interessato ha diritto di ottenere l'informazione sull'esistenza o meno di un trattamento di dati personali che lo riguardano, nonché l'accesso a tali dati personali ed ogni ulteriore informazione in relazione a: finalità del trattamento, origine e destinatario dei dati, la durata della conservazione dei dati personali e i suoi diritti.

Diritto alla rettifica

L'interessato ha diritto di ottenere senza ingiustificato ritardo la rettifica dei dati personali inesatti che lo riguardano.

Diritto alla cancellazione ("diritto all'oblio")

L'interessato può chiedere l'immediata cancellazione dei propri dati se, ad esempio, viene meno la finalità originaria del trattamento degli stessi, se viene revocato il consenso al trattamento, si oppone al trattamento o se i dati sono stati trattati illecitamente. Le eccezioni elencate nel GDPR devono essere osservate.

Diritto alla limitazione del trattamento

L'interessato può richiedere una limitazione del trattamento dei dati se questi, ad esempio, sono inesatti, utilizzati illecitamente o se è stato revocato il consenso al trattamento dei dati.

Diritto alla portabilità dei dati

L'interessato ha diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati o di farli trasmettere ad un altro controllore.

Diritto di opposizione

L'interessato può, in relazione a differenti finalità di utilizzo, opporsi al trattamento dei propri dati, in qualsiasi momento. Tale obiezione deve manifestarsi entro e non oltre il momento della prima comunicazione con l'interessato. Il diritto di opposizione deve essere portato esplicitamente a conoscenza dell'interessato e deve essere presentato in modo chiaro e separato da ogni altra informazione.

[7] Art. 12 et seq. GDPR

Notes

Protezione dei dati per tecnologia e organizzazione

Tenendo conto dello stato dell'arte, dei costi di attuazione, nonché della probabilità e del rischio per i diritti e le libertà dell'interessato, devono essere implementate misure tecniche e organizzative (TOM) appropriate per garantire la sicurezza dei dati.[8] A questo proposito, il livello di sicurezza dovrebbe essere commisurato alla gravità del rischio.

Il GDPR sottolinea l'importanza della protezione dei dati tecnici e organizzativi e ne attribuisce la responsabilità al titolare e al responsabile del trattamento.

Controller e responsabile della protezione dei dati

Il titolare del trattamento e il responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate al fine di garantire e poter dimostrare che il trattamento è conforme al presente regolamento.

Le aziende che trattano dati personali devono designare un responsabile della protezione dei dati in determinate circostanze.9 Questa persona deve possedere un elevato grado di competenza nel campo della protezione dei dati sulla base di qualifiche professionali o conoscenze specialistiche complete. È indispensabile la conoscenza dell'applicazione pratica delle normative sulla protezione dei dati.

Il nostro esperto consiglia

Nonostante il coinvolgimento di persone competenti, la responsabilità per l'attuazione della protezione dei dati e della sicurezza dei dati ai sensi del GDPR rimane alla direzione aziendale.

[8] Art. 5 (1) (f) e Art. 32 GDPR
[9] Art. 37 GDPR

Misure tecniche

Privacy by design

Misure tecniche per la sicurezza e la minimizzazione dei dati

È più facile rispettare la protezione dei dati se queste misure sono già state integrate nell'operazione di trattamento dei dati. Ciò influisce sulla selezione e sullo sviluppo di software e sistemi di elaborazione dati.

Privacy by default

Privacy per impostazione predefinita

Le preimpostazioni e le impostazioni predefinite dovrebbero essere progettate per garantire che vengano elaborati il minor numero possibile di dati personali. Questo ha lo scopo di supportare quegli utenti che sono tecnicamente meno esperti e sono ad es. non è propenso a modificare le impostazioni di protezione dei dati secondo i propri desideri.

Il nostro esperto consiglia

Una crittografia o pseudonimizzazione dei dati e anche la capacità tecnica di garantire la riservatezza, l'integrità nonché la disponibilità e la resilienza dei sistemi possono essere vantaggiosi o addirittura necessari.

Consiglio pratico per l'utente

- Assicurarsi che hardware e software corrispondano sempre allo stato dell'arte. Vale a dire, utilizzare le versioni correnti del prodotto nella misura in cui è ragionevole.
- In relazione alla generazione di lead, non arricchire semplicemente i profili dei clienti esistenti, ma considerare lo scopo dell'utilizzo in ciascun caso per determinare se è possibile o se devono essere cancellate informazioni e, in tal caso, quali informazioni devono essere cancellate.

Cosa devi fare in caso di violazione dei dati personali

Notifica di una violazione dei dati personali

Le violazioni dei dati personali devono essere segnalate all'autorità di controllo competente senza indebito ritardo, entro e non oltre 72 ore dalla sua conoscenza.[10]

Si applica un'eccezione quando è improbabile che la violazione comporti un rischio per i diritti e le libertà personali dell'interessato, ad es. attraverso un'adeguata crittografia dei dati personali.

Notifica all'interessato

Se la violazione dei dati personali può comportare un rischio elevato per i diritti e le libertà personali delle persone fisiche, il responsabile del trattamento comunica la violazione dei dati personali all'interessato senza indebito ritardo.

Data protection impact assessment

Le valutazioni d'impatto sono eseguite quando un tipo di trattamento di dati personali può comportare un rischio elevato per i diritti e le libertà delle persone fisiche. Il titolare del trattamento deve, prima del trattamento, effettuare una valutazione di impatto delle operazioni di trattamento rispetto alla protezione dei dati personali.[11] Ciò vale in particolare nel caso delle nuove tecnologie, in ragione della natura, dell'ambito, del contesto e delle finalità del trattamento.

Una valutazione d'impatto sulla protezione dei dati è necessaria, tra l'altro, anche nei casi di trattamento di dati particolarmente sensibili e di videosorveglianza estesa.

[10] Art. 33 et seq. GDPR
[11] Art. 35 GDPR

Data transfers

Particolare attenzione deve essere prestata alla trasmissione dei dati personali. Una trasmissione avviene quando i dati sono comunicati a terzi. In tale contesto, i terzi sono persone o enti diversi dal titolare del trattamento. Fanno eccezione l'interessato stesso e anche i responsabili del trattamento.

Una trasmissione avviene quando i dati sono comunicati a un soggetto terzo esterno, sia attraverso l'invio esplicito degli stessi sia attraverso una banca dati clienti di uso comune. Ciò vale anche in relazione a una società controllata oa qualsiasi altra società del gruppo.

Una trasmissione di dati personali a un paese terzo è ammissibile solo a determinate condizioni, come, tra l'altro, l'autorizzazione individuale e il consenso dell'interessato. L'intento è di garantire con questi mezzi che il livello di tutela delle persone fisiche garantito dal GDPR non venga pregiudicato.

Notes

Responsabilità e sanzioni

Multe elevate

Può diventare costoso e persino mettere in pericolo l'esistenza di un'azienda: le aziende che violano la protezione dei dati rischiano multe sostanziali che possono arrivare fino a 20 milioni di euro o fino al quattro percento delle vendite globali dell'intero gruppo dell'anno precedente, a seconda di quale sia la somma più alta.

Responsabilità per il danno

Qualsiasi titolare del trattamento coinvolto nel trattamento dei dati personali risponde dei danni causati da un trattamento non effettuato nel rispetto delle norme sulla protezione dei dati.[12]

Diritto al risarcimento

Il GDPR introduce anche una richiesta di risarcimento per gli interessati che subiscono danni materiali o immateriali.

Riepilogo di consigli pratici per l'utente

- Documenta ciò che modelli nel tuo CRM e per quale motivo.
- Archivia solo i dati di cui hai effettivamente bisogno: meno è di più!
- Definire una chiara struttura di autorizzazione per l'accesso ai dati.
- Documenta le tue fonti, ad esempio, da dove hai ricevuto i dati e/o le informazioni.
- Evitare record di dati "duplicati", ovvero la conservazione degli stessi dati in più luoghi.

[12] Art. 82 GDPR

In pratica:
Preparare il tuo CRM per conformarsi al GDPR

Le aziende lottano per stare al passo con le richieste di leggi e regolamenti sulla protezione dei dati che si sono rivelati quasi impossibili da gestire senza l'aiuto di un sistema CRM professionale. Le soluzioni CRM forniscono i requisiti tecnici per l'implementazione della protezione dei dati nella vostra azienda e offrono supporto in relazione a ulteriori misure organizzative.

Data collection and storage

La sfida relativa al contatto iniziale è la registrazione lecita dei dati dei clienti:

- Come posso registrare i dati correttamente?
- Quali dati possono essere archiviati?
- Quali dati devono essere conservati?
- Quali dati non possono essere archiviati affatto?

Le parole chiave sono **consenso, minimizzazione dei dati e finalità specificata.**

Possono essere registrati e conservati solo i dati necessari alla corretta gestione di un negozio giuridico.

L'origine dei dati e, se del caso, i dettagli di un'eventuale successiva trasmissione degli stessi devono essere registrati e archiviati per poter fornire le informazioni necessarie.

Il nostro esperto consiglia

Le soluzioni CRM **offrono supporto** nell'implementazione della protezione dei dati, ma non sostituiscono in alcun modo ulteriori misure tecniche e, in particolare, organizzative necessarie. Attraverso la loro attrezzatura tecnica di base e l'adattabilità definita dall'utente, le soluzioni CRM di CAS Software AG forniscono componenti importanti per quanto riguarda la **privacy by design** e la **privacy by default**.

Per ottenere il **consenso**, è utile l'uso di un modulo. Assicurati di utilizzare un linguaggio chiaro e semplice e assicurati che il consenso sia rilasciato volontariamente.

Il modulo deve contenere quanto segue:

- Quali dati verranno registrati?
- Per quali scopi?
- Origine/fonte del contatto?
- Quale canale di comunicazione può essere utilizzato?
- Riferimento alla normativa sulla protezione dei dati della tua azienda, unitamente ai dati di contatto del titolare del trattamento e, se del caso, del responsabile della protezione dei dati.

Il nostro esperto consiglia

Quando si utilizzano moduli elettronici, le caselle di controllo per il consenso devono essere vuote. Vale a dire, potrebbero non essere preselezionati.

Memorizza il consenso con la formulazione del consenso nel tuo CRM, idealmente in combinazione con (link a) l'indirizzo corrispondente. Ciò consentirà in un secondo momento di produrre una prova dal file del cliente che il cliente ha acconsentito alla memorizzazione e all'elaborazione dei suoi dati.

Practical user tips for recording addresses

- Usa le **procedure guidate** degli indirizzi per registrare gli indirizzi in modo rapido e semplice tramite copia e incolla: questo elimina gli errori di battitura
- **Aiuti all'input**, completamento automatico e i controlli di coerenza assicurano che gli indirizzi siano registrati in modo completo e corretto.
- Crea **campi** separati per tutte le informazioni da registrare nella misura in cui non sono già fornite nel tuo CRM, ad es. per l'indirizzo origine (fonte del contatto), data (data del primo contatto), contatto iniziale di (membro del personale), scopo (scopo specificato), canale di comunicazione consentito (canale), termine di cancellazione/data di cancellazione
- Con l'uso dei **campi obbligatori** ti assicuri che il tuo personale registri per intero tutte le informazioni rilevanti e obbligatorie relative a un cliente
- In linea con la minimizzazione dei dati, devono essere raccolti e archiviati solo i dati assolutamente necessari. Non definire campi obbligatori per dati non necessari..
- Sfrutta la flessibilità della tua soluzione CRM per presentare le informazioni relative a ciascun contatto in modo chiaro, se del caso, in vari registri, facilitando così l'inserimento dei dati semplice e veloce.
- Laddove viene utilizzata una soluzione CRM con **modulo questionario,** un questionario può anche guidare l'utente nella registrazione degli indirizzi o nel chiarire i desideri di contatto.
- Se il modulo del questionario offre anche **questionari online**, puoi farlo compilare anche dal cliente stesso. Di conseguenza, spetta a lei decidere quali dati vengono registrati e per quale scopo possono essere utilizzati.
- Idealmente, le risposte possono essere trasferite direttamente dal questionario al record di dati dell'indirizzo tramite la **connessione di campo.** In questo modo si evitano lavori inutili e possibili errori di trascrizione.

Notes

Utilizzo dei dati personali

Targeted direct marketing

Dopo che un indirizzo è stato correttamente registrato e memorizzato, il passo successivo è rivolgersi direttamente al cliente.
Il cliente può essere solo contattato

- se ha dato il suo consenso,
- tramite il canale di comunicazione consentito e
- per lo scopo consentito.

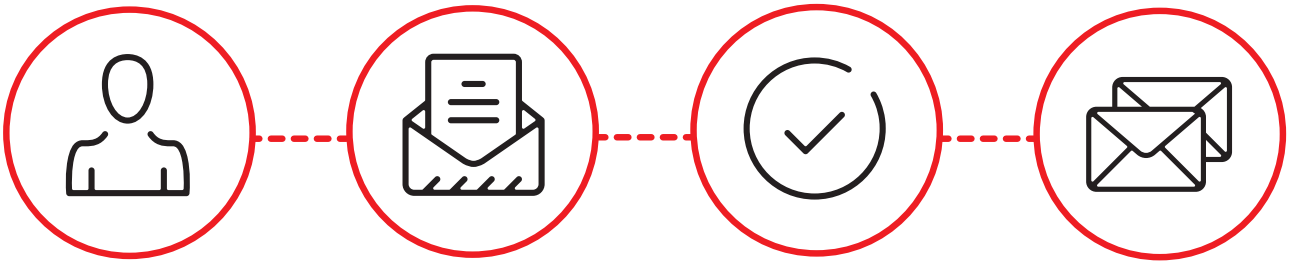
Al fine di ottenere l'autorizzazione per un contatto con il cliente appropriato, è prescritto il suo **consenso** (opt-in), in particolare in relazione al marketing diretto.

Al fine di evitare aggravamenti e malintesi, la semplice procedura di **opt-in** è sostituita dalla procedura di **double opt-in** in cui l'interessato deve confermare la propria adesione ad es. a una newsletter, in un secondo momento. A tal fine verrà inviata una e-mail all'indirizzo di contatto di posta elettronica registrato unitamente a una richiesta di conferma. Solo dopo l'arrivo della conferma la registrazione diventa effettiva.

Come ottenere il consenso per l'e-mail marketing

Per rispettare le disposizioni sulla protezione dei dati devi assicurarti di ricevere il consenso esplicito. L'utilizzo del **double-opt-in** è un buon modo per garantire la conformità e garantire il consenso nel tuo e-mail marketing.

1. Formulare una dichiarazione di consenso chiara e concisa nel modulo online. Dovrebbe contenere i seguenti punti:
   - Scopo d'uso, ad es. temi affrontati nel newsletter
   - Canale di comunicazione (e-mail, telefono, fax, SMS, lettera)
   - Contatti campi dati a seconda del canale di comunicazione: i campi obbligatori devono essere utilizzati solo per i dati di contatto essenziali, ad es. indirizzo e-mail per l'e-mail marketing
   - Dovresti includere un riferimento al Regolamento sulla protezione dei dati, nel corpo del testo o come link
   - Dovresti anche includere un riferimento al diritto i recesso: ricordando ai destinatari che possono revocare il consenso in qualsiasi momento
   - Casella di consenso: una volta che il destinatario contrassegna la casella di controllo e invia il modulo, acconsente al primo passaggio, ovvero la pubblicità (opt-in)
2. Invia al potenziale cliente un'e-mail all'indirizzo e-mail inserito nel modulo online, con il quale può confermare il proprio consenso. Il modo più semplice per farlo è includere un link di conferma nell'e-mail. **Nota:** l'e-mail di conferma non può contenere pubblicità o offerte.
3. Facendo clic sul collegamento nell'e-mail di richiesta di conferma di opt-in, il potenziale cliente conferma il proprio consenso a ricevere pubblicità via e-mail.



Opt-in del potenziale cliente | Collegamento di conferma | Conferma di iscrizione | Inserimento nella lista di distribuzione

Cosa bisogna tenere a mente in relazione alle diverse forme di marketing diretto?

Pubblicità via e-mail

Utilizzando il processo di opt-in è solitamente richiesto il consenso del cliente, contrariamente all'accordo di opt-out.

Ti consigliamo di utilizzare la procedura di double opt-in che offre una protezione aggiuntiva contro l'uso improprio.

Con ogni invio si richiama l'attenzione del destinatario sul suo diritto di revoca del proprio consenso e deve essere mostrato come può esercitare tale diritto di recesso.

In breve: ogni e-mail pubblicitaria deve contenere la possibilità di annullare l'iscrizione, idealmente tramite un collegamento di annullamento dell'iscrizione.

Pubblicità via telefono

Per il marketing diretto per telefono consigliamo l'accordo di opt-in. Il numero di telefono deve essere sempre visualizzato.

Pubblicità tramite fax

In caso di pubblicità via fax si applica la necessità del consenso.

Invii postali

Il marketing tramite posta è la forma tradizionale e più antica di marketing diretto. Prima di poter utilizzare i dati personali per il marketing postale, devi informare i clienti (o potenziali clienti) che intendi utilizzare i loro dati a tale scopo e dare loro l'opportunità di rifiutare tale utilizzo. È possibile contattare i destinatari purché non si siano opposti.

Se un cliente si oppone, non puoi utilizzare i suoi dati personali per commercializzarli direttamente. L'individuo può revocare il proprio consenso al marketing diretto in qualsiasi momento.

Il nostro esperto suggerisce

Prima di tutto, chiedi ai tuoi clienti e potenziali clienti già durante il contatto iniziale il loro consenso a ricevere mailing e newsletter e fallo confermare, ad es. secondo la procedura di double opt-in. Tenere presenti anche gli obblighi di documentazione e l'onere della prova ai sensi del GDPR.

Consigli pratici per l'utente per un contatto selettivo con i clienti

- Puoi **ottenere** il consenso in modo semplice utilizzando il **modulo questionario** nella tua soluzione CRM.
- Un questionario compilato positivamente serve come legittimazione per il marketing diretto. Archivia questo consenso nel tuo CRM, idealmente in **combinazione** con (link a) il record di dati dell'indirizzo corrispondente in modo da essere sempre in grado di fornire la prova che il consenso è stato concesso.
- Campi di indirizzo separati per il consenso e per il canale di comunicazione consentito/desiderato facilitano la selezione dei destinatari e la creazione di mailing list.
- Con un modulo di marketing nella tua soluzione CRM, hai generalmente possibilità complete per pianificare, implementare e valutare campagne multilivello: utilizzando mailing list e campagne, puoi indirizza i tuoi clienti secondo i loro desideri. I clienti vengono automaticamente assegnati al singolo canale di comunicazione di posta, e-mail ecc., in base a **campi** come "Metodo di contatto preferito" o "Metodo di contatto consentito". Se un determinato canale di contatto non è consentito, il CRM attirerà idealmente l'attenzione su questo fatto.
- Gli strumenti di e-mail marketing offrono anche possibilità convenienti ed efficaci di contatto con i clienti. In interazione con la soluzione CRM, gli indirizzi vengono forniti dal CRM e viene implementato professionalmente il mailing personalizzato. Successivamente, gli abbonamenti/disiscrizioni e anche i rimbalzi vengono ritrasmessi al CRM, in modo che gli indirizzi, insieme ai relativi consensi e alle mailing list, rimangano corrispondentemente aggiornati.
- Assicurati che in ogni campagna di e-mail marketing sia contenuto un **link di annullamento** dell'iscrizione.
- Creare il ruolo di una persona designata responsabile della gestione degli indirizzi e dei dati nella tua azienda.

Diritti del cliente

I diritti degli interessati sono espressamente rafforzati nel GDPR. Ad esempio, un cliente ha il diritto di far rettificare, bloccare o cancellare i propri dati. Inoltre, ha il diritto di ricevere gratuitamente informazioni su tutti i dati personali conservati – diritto alla portabilità dei dati, anche in un formato strutturato, di uso comune e leggibile da dispositivo automatico.

Il nostro esperto consiglia

L'obbligo di fornire informazioni pone le aziende di fronte a sfide importanti, in particolare quando i dati sono archiviati in luoghi separati e devono prima essere raccolti insieme. In questo caso, un'azione efficiente è essenziale per rispondere alle richieste in modo rapido e semplice. La maggiore consapevolezza delle questioni relative alla protezione dei dati può portare a un aumento del numero di richieste.

Consigli pratici per l'utente per rispettare i diritti dei clienti

- Il CRM è un ottimo, quasi indispensabile supporto nella documentazione dei dati dei clienti e nella registrazione, elaborazione e fruizione degli stessi. Una funzione di giornale può garantire che tutte le modifiche al record di dati dell'indirizzo vengano registrate senza interruzioni. Nel dossier cliente è possibile verificare quando l'indirizzo es. è stato aggiunto a quali mailing list, quali contatti e interazioni sono avvenuti e quali informazioni sono state inviate e quando.
- Utilizzando il dossier puoi tracciare e registrare quali dati sono stati trasmessi a chi e assicurarti di avere il consenso necessario per la trasmissione di tali dati.
- Con uno strumento per i report è possibile creare report con la semplice clic. Elencano tutti i dati memorizzati in relazione a una persona. Ciò ti consente di rispettare il diritto di qualsiasi persona all'informazione senza interruzioni e senza grandi spese.
- La maggior parte delle soluzioni CRM offre anche **funzioni di esportazione**, idealmente in vari formati di file. Ciò consente di rispettare il diritto di una persona alla portabilità dei dati.
- Se i dati devono essere rettificati o completati, può rivelarsi utile un **modulo questionario** con un questionario online.
- L'interessato ha il diritto di chiedere la rettifica, la cancellazione e/o il blocco del proprio indirizzo. Questa persona può vietare la diffusione e il trasferimento del proprio indirizzo. Soddisfa i desideri dei tuoi clienti impostando i **tags corrispondenti** nel CRM.

Data security

La sicurezza dei dati dei clienti include

- protezione contro il furto di dati,
- protezione contro l'abuso,
- protezione contro accessi non autorizzati.

Gli obiettivi di uno strumento software includono la semplificazione del lavoro per gli utenti. A tale scopo, il software offre molte funzioni utili. Tuttavia, se le funzioni vengono utilizzate in modo improprio, possono anche causare problemi.
Soprattutto nelle aree sensibili, è importante offrire funzioni efficienti e personalizzabili.

I meccanismi di sicurezza nelle soluzioni CRM aiutano a prevenire l'appropriazione indebita dei dati, in particolare l'esportazione o il trasferimento dei dati degli indirizzi personali. Ad esempio, le funzioni individuali come l'esportazione, i rapporti e l'utilizzo dei dati mobili dovrebbero essere collegate a diritti utente speciali che l'amministratore può chiudere completamente o rilasciare solo specificamente per i singoli dipendenti.

Contrapposto a questo, c'è tuttavia un desiderio di

- accesso flessibile ai dati tramite interfacce durante il viaggio,
- lavoro efficiente attraverso funzioni convenienti come drag & drop e
- adattabilità del sistema.

Ogni azienda deve trovare la propria soluzione ottimale tra questi due obiettivi opposti. Una protezione completa o al 100% contro il furto di dati e/o l'uso improprio non è tecnicamente possibile - tuttavia può essere notevolmente ostacolata.

Il nostro esperto consiglia

Chiedi al tuo personale di firmare una **dichiarazione sulla protezione dei dati** in cui chiarisce che i dati personali sono di proprietà dell'azienda e possono essere utilizzati solo per applicazioni definite e per scopi specifici in un ambito specifico.

Oltre alle misure tecniche e organizzative, definisci istruzioni dettagliate e **descrizioni di processo** per il tuo personale e addestralo alla preparazione, modifica e cancellazione dei record di dati. Comunica anche al tuo staff la pertinenza degli argomenti di cui sopra.

Consigli pratici per l'utente sulla sicurezza dei dati

- Il principio guida per le soluzioni CRM e anche per tutti gli altri sistemi è: Con **password e linee guida** crei un metodo efficace di controllo degli accessi.
- Creare **strutture di diritti** chiare e garantire il rispetto delle stesse. Più sofisticato e sviluppato è il sistema dei diritti della tua soluzione CRM, meglio è.
- Possibili livelli di diritti:
  - Diritti per gruppi di utenti, ad es. per reparti e livelli gerarchici
  - Diritti sui moduli, ad es. reportage e marketing
  - Diritti per funzioni, ad es. importazione ed esportazione e anchel'uso mobile di dati
  - Diritti individuali sui tipi di record di dati, ad es. opportunità di vendita
  - Diritti individuali a livello di campo, ad es. per i dati del personale
  - Diritti individuali su record di dati specifici, ad es. appuntamenti riservati
  - Diritti vari, dal diritto alla lettura fino ai pieni diritti
- Una documentazione dettagliata di un concetto di diritti garantisce chiarezza e trasparenza.
- Al fine di contenere le spese di amministrazione entro limiti, dovrebbe essere possibile modificare i diritti di più utenti contemporaneamente e adottare tutte le impostazioni dei privilegi nei processi di duplicazione.
- Dovrebbe anche essere possibile stabilire un diritto specifico alla cancellazione dei record di dati in modo che nessun dato possa essere cancellato in modo permanente, intenzionalmente o per errore. Per evitare errori, si consiglia di visualizzare un processo in due fasi sopra il cestino quando i dati devono essere cancellati.
- Cerca sigilli di qualità come "**Software made in Germany**" e in particolare "**Software hosted in Germany**". In particolare, le soluzioni software munite di quest'ultimo certificato non solo sono caratterizzate da alta qualità e fattibilità futura, ma sono anche ospitate in un data center in Germania soggetto alla legge tedesca sulla protezione dei dati.[13]

[13] The quality seals 'Software made in Germany' and 'Software hosted in Germany' are awarded by the Federal Association IT for Mediumsized Enterprises (BITMi e.V.), www.software-made-in-germany.org

Notes

Check list:
Cosa dovresti fare ora

Crea consapevolezza

Creare consapevolezza per la protezione dei dati all'interno della tua azienda: tutti all'interno della tua organizzazione o azienda devono conoscere le nuove disposizioni e le linee guida del GDPR dell'UE.

Gli imprenditori devono assicurarsi di aver fornito a tutti i dipendenti una guida chiara sui regolamenti e le procedure riguardanti le rispettive aree di responsabilità e far rispettare la due diligence. Ciò garantisce che la protezione dei dati sia rispettata in modo uniforme in tutta la vostra azienda.

Nomina un responsabile della protezione dei dati e coinvolgerlo nell'implementazione

Se, di norma, almeno nove membri del personale sono interessati al trattamento dei dati personali, è necessario designare formalmente un responsabile della protezione dei dati.

Il responsabile della protezione dei dati controlla e regola l'attuazione delle disposizioni sulla protezione dei dati nella vostra azienda. È molto importante che qualcuno nella tua organizzazione si assuma la responsabilità adeguata della conformità alla tua protezione dei dati e abbia le conoscenze, il supporto e l'autorità per svolgere il proprio ruolo in modo efficace.

Qualsiasi soggetto della società può essere nominato responsabile della protezione dei dati se possiede la necessaria competenza professionale in materia di protezione dei dati o la acquisisce attraverso programmi di formazione e/o perfezionamento.

Revisionare i tuoi dati personali

Dovresti rivedere tutti i dati personali che hai già nella tua azienda e documentare quanto segue:

- Il tipo di dati personali che hai memorizzato – questo include sia i dati dei clienti che i dati del personale,
- la fonte dei dati,
- lo scopo per il quale i dati sono stati raccolti e conservati
- nonché la posizione dei dati memorizzati e i dettagli su quanto tempo devono essere conservati.

Se necessario, eseguire una pulizia dei dati in cui vengono conservati solo i dati necessari per le finalità specificate. Gli altri dati dovrebbero essere cancellati.

Creazione di un elenco delle procedure/ elenco delle attività di trattamento

Se non è già in atto, predisporre un elenco delle procedure sotto forma di tabella e trasmetterlo alle autorità di vigilanza. La tabella dovrebbe elencare quali dati sono stati raccolti nella tua azienda, nonché quando, come e perché. Si prega di notare che è importante includere i dati del personale interno e i dati dei clienti.

Ciascun dipartimento all'interno della tua azienda dovrebbe creare una tabella contenente descrizioni procedurali che affrontino i seguenti argomenti:

- Tipo o categoria di dati (es. indirizzo, CV, dati account, ecc.)
- Finalità del trattamento dei dati (es. gestione delle assunzioni, marketing ecc.)
- Data in cui i dati sono stati raccolti
- Informativa resa all'interessato in merito alla raccolta, conservazione ed elaborazione dei suoi dati
- Consenso dell'interessato
- Destinatario/Titolare (che ha accesso ai dati)
- Cancellazione e scadenze di cancellazione
- Procedura per l'informativa all'interessato e contenuto della presente informativa
- Conversione dei dati in un altro formato ai fini della portabilità dei dati
- Periodo di conservazione dei dati (se i dati non vengono utilizzati
- Misure tecniche e organizzative relative alla protezione dei dati (tra l'altro, pseudonimizzazione)
- Misure tecniche e organizzative relative alla protezione dei dati (tra l'altro, pseudonimizzazione)

Inoltre, dovresti documentare l'intero percorso dei dati personali, dalla loro raccolta alla loro conservazione fino all'utilizzo dei dati.

Definisci i tuoi processi e crea un manuale di processo

Documenta tutte le procedure della tua azienda connesse al trattamento dei dati e adattale, se necessario, alla conformità con le linee guida sulla protezione dei dati.

Tipicamente, questi processi includono, tra le altre cose:

- Il modo in cui le richieste vengono gestite nell'ambito dei diritti dell'interessato, compresi gli obblighi di fornire informazioni,
- La procedura di documentazione e l'obbligo di dimostrare il rispetto degli obblighi in materia di trattamento dei dati,
- e anche la notifica di violazioni della protezione dei dati. In questo caso, dovresti considerare sia il trattamento tecnico che il comportamento del tuo personale.

Valutazione dell'impatto sulla protezione dei dati

Qualsiasi persona che lavori con dati particolarmente sensibili deve trattarli con eccezionale cura e, in determinate circostanze, eseguire una cosiddetta valutazione d'impatto sulla protezione dei dati. Serve alla tua azienda come misura precauzionale che puoi utilizzare per valutare eventuali rischi per i diritti personali degli interessati durante il trattamento dei loro dati. Inoltre, consente di pianificare e attuare misure di protezione adeguate.

Questo è particolarmente vero per quelle aziende che elaborano informazioni sensibili come ad es. informazioni riguardanti la salute, le finanze, le affinità etniche e l'affiliazione politica.

Consenso

Verifica come la tua azienda ottiene, archivia e gestisce il consenso al trattamento dei dati. Ciò si estende a tutte le procedure e moduli utilizzati. Se i processi attualmente implementati non sono conformi alle disposizioni in materia di protezione dei dati, è necessario adattare le procedure e i relativi moduli. Se necessario, rinnovare eventuali consensi esistenti.

Pianifica, controlla e documenta i TOM

Se non li stai già utilizzando, dovresti introdurre nella tua azienda misure tecniche e organizzative (TOM) per rispettare le disposizioni sulla protezione dei dati. Oltre alle misure tecniche "privacy by design" e "privacy by default", misure appropriate comprendono la pseudonimizzazione e la crittografia dei dati e anche l'introduzione di rigorose strutture di autorizzazione all'accesso ai dati.

Notes

Conclusione

In questa guida abbiamo considerato le disposizioni sulla protezione dei dati che hanno un impatto particolare sulla gestione delle relazioni con i clienti. Abbiamo anche cercato di dimostrare come è possibile utilizzare il CRM per soddisfare le importanti richieste del GDPR e implementare ulteriori leggi.

Affronta in modo approfondito il tema della protezione dei dati, controlla i tuoi dati esistenti e anche tutti i processi relativi ai dati personali dei clienti Utilizzali per elaborare misure di protezione dei dati adeguate che soddisfino le esigenze individuali della tua azienda.

Parla con il tuo responsabile della protezione dei dati ed elabora un manuale per la protezione dei dati nella tua azienda.

Le aziende senza CRM avranno difficoltà a rispettare la protezione dei dati. L'utilizzo di una soluzione CRM di CAS Software AG vi darà un indubbio vantaggio nel rispetto delle normative.

In questo modo accetti la sfida della protezione dei dati e sfrutta le opportunità che offre.
Vi auguriamo ogni successo e speriamo che le vostre relazioni con i clienti continuino a prosperare.

Cordiali Saluti
CAS Software
AG www.cas.de

In collaorazione con:

Thomas Heimhalt
DATENSCHUTZ *perfect* GbR
Data protection consultant, responsabile e revisore (TÜV) www.datenschutz-perfect.de

Contatto

CAS Software AG
CAS-Weg 1-5
76131 Karlsruhe, Germany
Telefono: +49 721 9638-188
E-mail: crm@cas.de
www.cas-crm.com