Vanderbilt SPC

Regolamento generale UE sulla protezione dei dati personali – Guida alla conformità

Indice

Sommario

Le soluzioni e i prodotti Vanderbilt consentono ai clienti di gestire e trattare i dati personali in modo compatibile con i requisiti GDPR. Questa guida nasce con lo scopo di aiutare e supportare i nostri clienti nella valutazione della loro prontezza ad adempiere agli obblighi e alle responsabilità derivanti dalla nuova normativa.

Panoramica generale

La protezione dei dati è un diritto fondamentale e in quanto tale tutti hanno il diritto a proteggere i propri dati personali. Il regolamento generale sulla protezione dei dati (GDPR) è in vigore dal 25 maggio 2018 ed è stato concepito per dare agli individui un maggiore controllo sui propri dati personali. Si tratta di un complesso unico di regole valido per l'intera UE che la legislazione nazionale può integrate in alcuni specifici ambiti.

Il GDPR impone obblighi a imprese e organizzazioni che raccolgono, utilizzano e trattano dati personali. Al centro del GDPR vi è l'obbligo per le organizzazioni e le imprese ad assicurare piena trasparenza sulle modalità con cui usano e proteggono i dati personali e di dimostrare di aver responsabilmente adottato comportamenti proattivi per il trattamento dei dati tali da assicurare l'applicazione del regolamento. I dati devono essere trattati in modo corretto, per finalità determinate e con il consenso della persona interessata o in base a specifiche motivazioni stabilite dalla legge.

Sebbene Vanderbilt offra ai clienti nei suoi prodotti funzioni flessibili e intuitive per facilitare la conformità con il nuovo regolamento, l'organizzazione Vanderbilt non raccoglie, controlla, utilizza o tratta i dati personali esistenti all'interno dei prodotti Vanderbilt sui sistemi locali dei clienti. È quindi pertanto compito e responsabilità del titolare del trattamento e del responsabile del trattamento dei dati personali garantire il rispetto degli obblighi stabiliti dal GDPR.

In caso di dubbi o di incertezza su chi si ad avere il ruolo di titolare e/o responsabile del trattamento, consultare il proprio consulente legale.

Che cosa sono i dati personali?

Con il termine "dati personali" si intende qualsiasi informazione relativa a una persona vivente identificata o identificabile.

Una persona è identificabile se può essere identificata direttamente o indirettamente tramite un "identificatore". Il GDPR fornisce esempi di identificatori, come nomi, numeri di identificazione e dati sulla posizione. Una persona può anche essere identificabile tramite riferimento a fattori che sono specifici della sua identità, come fattori fisici, genetici o culturali.

I dati personali sottoposti a deidentificazione, cifratura o pseudonimizzazione, ma che possono essere utilizzati per reidentificare una persona, rimangono dati personali e rientrano nell'ambito di applicazione della normativa. I dati personali che sono stati resi anonimi, in modo tale che l'individuo non sia o non sia più identificabile, non sono più considerati dati personali. Perché i dati siano veramente anonimi, l'anonimizzazione deve essere irreversibile.

La legge protegge i dati personali indipendentemente dalla tecnologia o dal metodo utilizzato per il trattamento di tali dati e si applica sia al trattamento automatizzato che a quello manuale. Inoltre,

non importa come i dati vengono archiviati: in un sistema informatico, tramite videosorveglianza o su carta; in tutti questi casi, i dati personali sono soggetti agli obblighi di protezione stabiliti nel regolamento.

Cosa si intende per trattamento dei dati?

Il trattamento dei dati copre una vasta gamma di operazioni eseguite sui dati personali, con mezzi manuali o automatizzati. Include la raccolta, la registrazione, l'organizzazione, la strutturazione, la memorizzazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione dei dati.

Il Regolamento generale sulla protezione dei dati (GDPR) si applica al trattamento dei dati personali eseguito sia in tutto o in parte mediante strumenti automatizzati che mediante trattamento non automatizzato, se parte di un sistema di archiviazione strutturato.

Sono il titolare del trattamento o il responsabile del trattamento?

Il titolare del trattamento è l'individuo o la persona giuridica che controlla e ha la responsabilità per la conservazione e l'uso delle informazioni personali memorizzate su sistemi informatici o in archivi non automatizzati strutturati. Il ruolo di titolare del trattamento comporta responsabilità legali ed è quindi necessario essere certi se queste responsabilità ricadono su sé stessi o la propria organizzazione.

Se lei o la sua organizzazione siete ad avere il controllo e la responsabilità per i dati personali che detenete, cioè se siete voi a decidere quali informazioni personali conservare e per quali finalità, allora siete lei o la sua organizzazione a essere il titolare del trattamento.

Esempi di casi in cui il titolare del trattamento dei dati è un individuo: medici generici, farmacisti, politici e ditte individuale poiché questi conservano dati personali sui loro pazienti, clienti, elettori, ecc.

Se lei o la sua organizzazione detenete i dati personali, ma sono altri individui o organizzazioni a decidere e avere la responsabilità per ciò che accade ai dati, allora sono questi altri soggetti o organizzazioni a essere il titolare del trattamento dei dati e lei o la sua organizzazione siete il "responsabile del trattamento".

Come esempi di responsabili del trattamento possiamo indicare le società che si occupano dell'elaborazione delle buste paga, i contabili e le società di ricerche di mercato, che possono detenere o trattare dati personali per conto di qualcun altro.

Che cos'è il consenso ai dati e devo tenerlo in considerazione?

Per poter trattare lecitamente i dati personali, le organizzazioni e le imprese devono sin dall'inizio identificare e documentare la base legale che le autorizza a farlo. Alcuni dei modi legali per trattare i dati includono:

- **Consenso dell'individuo:** il consenso è appropriato se alla persona viene offerta una reale possibilità di scelta e di controllo sull'uso dei suoi dati.
- **Interessi vitali:** il trattamento è necessario per proteggere gli interessi vitali dell'individuo, per esempio se è necessario proteggere la vita di qualcuno.

- **Conformità a obbligo di legge:** i dati possono essere trattati se, per esempio, ciò è richiesto dalla normativa UE per uno scopo preciso.
- **Contratto con l'individuo:** il trattamento è necessario per dare esecuzione a un contratto con l'individuo, per esempio per fornire beni o servizi che sono stati richiesti

Se non si è certi di disporre di sufficiente consenso al trattamento dei dati personali, rivolgersi al proprio consulente legale.

Che cos'è un contratto per il trattamento dei dati e devo tenerlo in considerazione?

Se si detengono o trattano (inserimento, modifica, mantenimento) dati personali (responsabile del trattamento) per conto del cliente (titolare del trattamento) è necessario un contratto che regoli il trattamento dei dati. Raccomandiamo di rivolgersi a un consulente legale per garantire che il contratto sia conforme ai requisiti di sicurezza e di protezione dei dati personali. In qualità di parte interessata raccomandiamo ai clienti di predisporre una lista di controllo riguardante la gestione dei dati e la consegna del sistema di sicurezza.

Conoscere il proprio ruolo e le proprie responsabilità

È chiaro che la legislazione si sta adeguando al nuovo regolamento e ciò deve essere tenuto in considerazione nella pianificazione dei sistemi di sicurezza. È necessario identificare e affrontare gli aspetti che possono causare problemi di conformità ai sensi del regolamento. Il regolamento GDPR assicura alle persone il diritto a ricevere informazioni chiare sull'uso dei loro dati personali.

Il primo passo è identificare il proprio ruolo e le proprie responsabilità secondo i termini del regolamento. Lei è il titolare o il responsabile del trattamento oppure ricopre entrambi i ruoli? In caso di dubbi o di incertezza su chi si ad avere il ruolo di titolare e/o responsabile del trattamento, consultare il proprio consulente legale.

Il secondo passo è assicurare la responsabilizzazione. Consideriamo l'insieme dei dati personali che vengono trattati durante il funzionamento di un sistema di sicurezza ed esaminiamoli tenendo conto dei seguenti fattori:

- Che tipo di dati personali vengono memorizzati?
- Qual è la base giuridica del trattamento dei dati personali?
- Dove sono archiviati i dati?
- Come vengono protetti i dati?
- Per quanto tempo vengono conservati i dati?
- Quali sono le procedure di gestione delle richieste di accesso ai dati presentate dei soggetti interessati?
- Qual è la procedura da seguire se un soggetto chiede di essere rimosso dal sistema?
- Chi ha accesso ai dati?
- I dati personali vengono trasferiti al di fuori del spazio economico europeo?

SPC & GDPR

Le informazioni che seguono descrivono come utilizzare i controllori serie SPC di Vanderbilt per facilitare la conformità GDPR.

Che tipo di dati personali vengono memorizzati?

Gli utenti di SPC devono inserire le seguenti informazioni obbligatorie durante la procedura di registrazione:

- Nome utente
- PIN

Durante il funzionamento di SPC Connect, le seguenti informazioni possono essere associate agli account utente.

- Password web
- Numero scheda

Qual è la base giuridica del trattamento dei dati personali?

Il controllore SPC è un elemento funzionale del sistema, l'inserimento e il mantenimento dei dati sono controllati dal titolare del trattamento e dal responsabile del trattamento del sito. È quindi responsabilità del titolare del trattamento e/o del responsabile del trattamento assicurare la base legale che autorizza il trattamento dei dati personali.

I dati dell'utente sono inseriti nel sistema

- dall'amministratore ("Installatore")
- un utente che ha ricevuto i permessi dall'amministratore.

Dove sono archiviati i dati?

Tutti i dati SPC sono memorizzati nel controllore SPC in formato compresso e l'accesso al file è limitato all'amministratore ("installatore") del sistema. Solo l'utente amministratore può accedere a questo file.

Come vengono protetti i dati?

L'accesso ai dati SPC è protetto in modo tale che solo l'amministratore ("installatore") possa accedervi. Il normale funzionamento prevede che l'amministratore conceda accesso all'utente il che vuol dire una procedura di protezione in due fasi.

Per quanto tempo vengono conservati i dati?

I dati dell'utente sono conservati fino a quando non sono rimossi dall'amministratore del sistema. È responsabilità dell'amministratore del sistema comunicare in modo trasparente la durata del periodo di conservazione dei dati.

Quali sono le procedure di gestione delle richieste di accesso ai dati presentate dei soggetti interessati?

Se viene inoltrata una richiesta, è responsabilità del titolare del trattamento e/o del responsabile del trattamento delineare la procedura e fornire i dati in modo tempestivo e in conformità al regolamento GDPR.
Il nome dell'utente e il numero della scheda possono essere rilevati dal sistema SPC dagli utenti che dispongono di sufficienti diritti.

Qual è la procedura da seguire se un soggetto chiede di essere rimosso dal sistema?

Se viene inoltrata una richiesta, è responsabilità del titolare del trattamento e/o del responsabile del trattamento delineare la procedura e rimuovere i dati in modo tempestivo e in conformità al regolamento GDPR.
Gli account utente possono essere cancellati dal sistema rimuovendo nome utente, PIN e scheda dal sistema SPC.

Chi ha accesso ai dati?

È responsabilità del titolare del trattamento e/o del responsabile del trattamento rivelare chi ha accesso ai dati personali sul sistema SPC installato nel sito. Vanderbilt non ha accesso e/o la possibilità di trattare dati personali nei sistemi SPC in loco.

I dati personali vengono trasferiti al di fuori del spazio economico europeo?

I dati degli utenti non sono condivisi all'esterno del sistema SPC nel suo normale funzionamento. È responsabilità del titolare del trattamento e/o del responsabile del trattamento rivelare se il sistema è configurato in modo tale da trasferire dati al di fuori dello spazio economico europeo.