



# Vanderbilt ACT Enterprise

## Datenschutz-Grundverordnung der EU – Ein Compliance-Leitfaden

### Inhalt

Zusammenfassung.....	2
Überblick .....	2
Was sind personenbezogene Daten?.....	2
Was ist mit Datenverarbeitung gemeint? .....	3
Bin ich ein Datenkontrolleur oder Datenverarbeiter? .....	3
Was ist eine Einwilligungserklärung, und wofür ist sie gedacht? .....	3
Was ist ein Datenverarbeitungsvertrag, und wofür ist er gedacht? .....	4
Kennen Sie Ihre Rolle und Pflichten .....	4
ACT Enterprise und die DSGVO .....	5



## Zusammenfassung

Die Lösungen und Produkte von Vanderbilt ermöglichen es Kunden, personenbezogene Daten so zu verwalten und zu verarbeiten, wie dies in der DSGVO vorgeschrieben ist. Dieser Leitfaden soll unseren Kunden dabei behilflich sein, ihre eigene Fähigkeit zur Einhaltung ihrer Verantwortlichkeiten und Pflichten in Hinsicht auf das neue Gesetz zu bewerten.

## Überblick

Datenschutz ist ein grundlegendes Recht – jeder hat Anspruch darauf, dass die Daten zur eigenen Person geschützt werden. Die Datenschutz-Grundverordnung (DSGVO) tritt am 25. Mai 2018 in Kraft und soll Einzelpersonen größere Kontrolle über ihre personenbezogenen Daten geben. Für die gesamte EU gilt ein einziger Regelsatz, der in manchen Bereichen durch die Gesetzgebung der einzelnen Länder ergänzt werden kann.

Die DSGVO erlegt Unternehmen oder Organisationen, die personenbezogene Daten erfassen, nutzen und verarbeiten bestimmte Pflichten auf. Der Schwerpunkt der DSGVO ist die Verpflichtung von Organisationen und Unternehmen, in Bezug auf die Nutzung und den Schutz personenbezogener Daten vollständig transparent zu sein. Außerdem müssen Sie einen verantwortlichen Umgang mit der Datenverarbeitung nachweisen können. Solche Daten müssen auf faire Art und Weise zu einem bestimmten Zweck und auf Grundlage der Einwilligung der betroffenen Person oder auf einer anderen gesetzlich festgelegten Grundlage verarbeitet werden.

Zwar bietet Vanderbilt Kunden eine flexible und intuitive Produktfunktionalität, die die Einhaltung der Gesetzesneuerungen erleichtert, aber das Unternehmen Vanderbilt erfasst, kontrolliert, nutzt oder verarbeitet keine personenbezogenen Daten, die auf ortsgebundenen Produkten von Vanderbilt gespeichert werden. Es liegt daher in der Pflicht des Kontrolleurs und Verarbeiters personenbezogener Daten, sicherzugehen, dass die Auflagen der DSGVO eingehalten werden.

Falls Sie Zweifel haben oder sich über die Identität des Datenkontrolleurs und/oder Datenverarbeiters nicht sicher sind, sollten Sie sich an Ihren Rechtsbeistand wenden.

## Was sind personenbezogene Daten?

Der Begriff „personenbezogene Daten“ bezieht sich auf Daten zu einer lebenden Person, die durch diese identifiziert wird oder identifizierbar ist.

Eine Person ist dann identifizierbar, wenn sie direkt oder indirekt anhand eines „Identifikators“ identifiziert werden kann. In der DSGVO sind Beispiele für Identifikatoren angegeben, wie Namen, Identifikationsnummern und Standortdaten. Eine Person kann auch mittels Verweis auf Merkmale identifizierbar sein, die spezifisch für deren Identität sind, wie beispielsweise körperliche, genetische oder kulturelle Merkmale.

Personenbezogene Daten, die ent-identifiziert, verschlüsselt oder pseudonymisiert worden sind, aber verwendet werden können, um eine Person zu re-identifizieren, sind nach wie vor personenbezogene Daten und fallen unter die DSGVO. Sind personenbezogene Daten so anonymisiert worden, dass die Person nicht mehr identifizierbar ist, gelten sie nicht als personenbezogene Daten. Damit Daten tatsächlich anonymisiert sind, muss die Anonymisierung irreversibel sein.



Das Gesetz schützt personenbezogene Daten ungeachtet der für die Verarbeitung der Daten verwendeten Technologie oder Methode – es bezieht sich sowohl auf die automatisierte als auch die manuelle Verarbeitung. Es spielt außerdem keine Rolle, wie die personenbezogenen Daten gespeichert werden – in einem IT-System, mittels Videoüberwachung oder auf Papier. In jedem Fall unterliegen die personenbezogenen Daten den in der DSGVO festgelegten Auflagen zur Geheimhaltung.

## Was ist mit Datenverarbeitung gemeint?

Die Verarbeitung bezieht sich auf ein breites Spektrum an Verfahren, die an personenbezogenen Daten durchgeführt werden, u. a. durch manuelle und automatisierte Methoden. Dazu gehören die Erfassung, Aufzeichnung, Organisation, Strukturierung, Speicherung, Anpassung oder Änderung, der Abruf, die Absprache, die Nutzung, die Weitergabe durch Übertragung, Verteilung oder anderweitige Verfügbarmachung, Ausrichtung oder Kombination, Einschränkung, Löschung oder Vernichtung personenbezogener Daten.

Die Datenschutz-Grundverordnung (DSGVO) findet auf die gänzliche oder teilweise Verarbeitung personenbezogener Daten mittels automatisierter Methoden sowie nicht-automatisierter Methoden, sofern sie Teil eines strukturierten Ablagesystems bildet.

## Bin ich ein Datenkontrolleur oder Datenverarbeiter?

Ein Datenkontrolleur ist die Person oder Rechtsperson, die die personenbezogenen Daten kontrolliert und für die Vorratsspeicherung und Nutzung personenbezogener Daten auf Computern oder in strukturierten manuellen Akten zuständig ist. Die Aufgabe des Datenkontrolleurs bringt bestimmte rechtliche Pflichten mit sich; Sie sollten sich daher unbedingt darüber im Klaren sein, ob diese Pflichten für Sie oder Ihr Unternehmen gelten.

Wenn Sie oder Ihr Unternehmen für die personenbezogenen Daten verantwortlich sind bzw. ist, die sich in Ihrem bzw. seinem Besitz befinden, d. h. Sie entscheiden bzw. es entscheidet, welche personenbezogenen Daten verwahrt und wie diese genutzt werden, sind Sie oder Ihr Unternehmen ein Datenkontrolleur.

Beispiele für Fälle, in denen der Datenkontrolleur eine Einzelperson ist, sind Allgemeinärzte, Apotheker, Politiker und Einzelunternehmer. Hier werden personenbezogene Daten zu Patienten, Kunden, Inhaltsstoffen usw. verwahrt.

Wenn Sie oder Ihr Unternehmen die personenbezogenen Daten halten bzw. hält, jedoch eine andere Person oder ein anderes Unternehmen entscheidet und dafür verantwortlich ist, wie mit den Daten umgegangen wird, ist die andere Person bzw. das andere Unternehmen der Datenkontrolleur, und Sie oder Ihr Unternehmen sind ein „Datenverarbeiter“.

Beispiele für Datenverarbeiter sind Payroll-Unternehmen, Buchhalter und Marktforschungsagenturen, die personenbezogene Daten im Auftrag von jemand anderem verwahren oder verarbeiten können.

## Was ist eine Einwilligungserklärung, und wofür ist sie gedacht?

Um personenbezogene Daten legal verarbeiten können, müssen Organisationen und Unternehmen von Anfang an die Rechtsgrundlage hierfür angeben und dokumentieren. Einige der Methoden, um die Rechtmäßigkeit der Verarbeitung von Daten sicherzustellen, sind:



- **Einwilligung der Einzelperson:** Die Einwilligung ist dann wirklich angemessen, wenn der betreffenden Person eine echte Wahl und Kontrolle darüber gegeben wurde, wie ihre Daten genutzt werden.
- **Lebenswichtige Interessen:** Die Verarbeitung ist nötig, um die lebenswichtigen Interessen der Einzelperson zu wahren, z. B. wenn das Leben von jemandem auf dem Spiel steht.
- **Compliance infolge einer gesetzlich vorgeschriebenen Pflicht:** Daten können verarbeitet werden, wenn dies z. B. von der EU für einen bestimmten Zweck vorgeschrieben ist.
- **Ein Vertrag mit der Einzelperson:** Die Verarbeitung ist für die Erfüllung eines Vertrages mit einer Einzelperson erforderlich, z. B. um bestellte Ware zu liefern oder in Auftrag gegebene Dienstleistungen zu erbringen.

Falls Sie sich nicht sicher sind, ob die eingeholte Einwilligung für die Verarbeitung personenbezogener Daten ausreicht, sollten Sie Ihren Rechtsbeistand um Rat bitten.

## Was ist ein Datenverarbeitungsvertrag, und wofür ist er gedacht?

Wenn Sie personenbezogene Daten (Datenverarbeiter) im Auftrag Ihres Kunden (Datenkontrolleurs) verarbeiten (eingeben, bearbeiten, pflegen), benötigen Sie einen Datenverarbeitungsvertrag. Wir empfehlen Ihnen, den Rat eines Rechtsanwalts einzuholen, um sicherzugehen, dass angemessene Sicherheits- und sonstige Datenschutzvorkehrungen angewendet werden. Wir empfehlen Kunden, eine Checkliste bezüglich der Handhabung von Daten und der Übergabe des Sicherheitssystems zu führen.

## Kennen Sie Ihre Rolle und Pflichten

Von nun an gilt die DSGVO, die bei der Planung von Sicherheitssystemen berücksichtigt werden muss. Es gilt, Bereiche, die unter der DSGVO zu Compliance-Problemen führen könnten, zu identifizieren und entsprechend anzupassen. Gemäß DSGVO haben Einzelpersonen Anspruch auf klare Informationen darüber, wie ihre Daten genutzt werden.

Der erste praktische Schritt ist es, Ihre Rolle und Pflichten in Hinsicht auf die DSGVO festzulegen. Sind Sie Datenkontrolleur oder Datenverarbeiter oder beides? Falls Sie Zweifel haben oder sich über die Identität des Datenkontrolleurs und/oder Datenverarbeiters nicht sicher sind, sollten Sie sich an Ihren Rechtsbeistand wenden.

Der zweite Schritt ist es, pflichtbewusst zu werden. Denken Sie an die personenbezogenen Daten, die Sie bei der Arbeit mit dem Sicherheitssystem handhaben, und denken Sie über folgende Gesichtspunkte nach:

- Welche personenbezogene Daten werden gespeichert?
- Auf welcher Rechtsgrundlage beruht die Verarbeitung personenbezogener Daten?
- Wo werden die Daten gespeichert?
- Wie werden die Daten geschützt?
- Wie lange werden die Daten gespeichert?
- Welche Richtlinie gibt es für den Umgang mit einzelnen Datenzugriffsanfragen?
- Wie geht man vor, wenn jemand beantragt, aus dem System entfernt zu werden?
- Wer hat Zugriff auf die Daten?
- Werden personenbezogene Daten außerhalb des EWR übertragen?



## ACT Enterprise und die DSGVO

Im Folgenden wird beschrieben, wie das ACT Enterprise-System von Vanderbilt dazu beitragen kann, dass die Auflagen der DSGVO eingehalten werden.

### Welche personenbezogene Daten werden gespeichert?

Für die ordnungsgemäße Funktion des ACT Enterprise-Systems ist die Speicherung personenbezogener Daten nicht zwingend erforderlich.

Zwar sind Foto, Name, E-Mail-Adresse und Telefonnummer im System als Felder vordefiniert, es können jedoch benutzerdefinierbare Felder für die Eingabe verschiedener personenbezogener Daten verwendet werden.

### Auf welcher Rechtsgrundlage beruht die Verarbeitung personenbezogener Daten?

Die Eingabe und Pflege von Daten wird vom Datenkontrolleur und Datenverarbeiter des Standorts kontrolliert. Somit obliegt es dem Datenkontrolleur und/oder Datenverarbeiter, dafür zu sorgen, dass die Rechtsgrundlage für die Verarbeitung personenbezogener Daten gegeben ist.

Die ACT Enterprise-Software ist nicht mit speziellen Verfahren für den Erhalt oder die Aufzeichnung der Einwilligung des Benutzers ausgestattet.

### Wo werden die Daten gespeichert?

Die Daten werden in der ACT Enterprise-Datenbank auf dem Server und in Sicherungskopien gespeichert. Zwar können bestimmte personenbezogene Daten in den Systemcontrollern gespeichert werden (Namen), diese Funktion kann jedoch vom Systemeigentümer deaktiviert werden.

### Wie werden die Daten geschützt?

Für den Zugriff auf den Inhalt der ACT Enterprise-Datenbank wird die Client-Software (ACT Manage, Monitor oder Install) verwendet. Bei der Anmeldung ist die Software passwortgeschützt.

Wir verschlüsseln keine personenbezogenen Daten. Der Endbenutzer kann sich dafür entscheiden, auf Datenbank-Ebene (SQL Server oder SQL Compact) eine Verschlüsselung zu erzwingen.

Die Mitarbeiter von Vanderbilt haben keinen Zugriff auf das System des Kunden, sofern er nicht mittels Remote-Anmeldung gewährt wird.

### Wie lange werden die Daten gespeichert?

In ACT Enterprise werden die Daten des Karteninhaber so lange gespeichert, wie dieser eine Karte benötigt. Zwar kann ein Ablaufdatum für die Karte festgelegt werden, der Systembenutzer muss sich jedoch nach Ablauf der Karte um die Löschung des Karteninhabers kümmern. Vanderbilt kann diesen Prozess bei Bedarf mit einem Kartenablaufbericht vereinfachen.

Wir bieten eine Funktion, über die Protokollereignisse, die älter als eine bestimmte Anzahl von Monaten sind, automatisch gelöscht werden. Dies ist vom Benutzer konfigurierbar. Gemäß Voreinstellung werden Ereignisse unbegrenzt gespeichert.

Nach dem Löschen eines Karteninhabers löscht das System nicht automatisch auch dessen entsprechenden Protokollereignisse. Dies kann jedoch so geändert werden, dass die Protokollereignisse gelöscht werden, wenn der Benutzer gelöscht wird.



## Welche Richtlinie gibt es für den Umgang mit einzelnen Datenzugriffsanfragen?

Bei entsprechender Anfrage haben der Datenkontrolleur und/oder die Datenverarbeiter auf die Richtlinie hinzuweisen und die Daten fristgemäß und in Übereinstimmung mit den Bestimmungen der DSGVO bereitzustellen.

In ACT Enterprise können verschiedene Berichte mit den zu einer Person gespeicherten Daten erstellt werden, u. a. ein Bericht mit den neuesten Protokollereignissen. Diese Daten können in Standard-PDF-Berichte oder CSV-Dateien exportiert werden.

## Wie geht man vor, wenn jemand beantragt, aus dem System entfernt zu werden?

Bei entsprechender Anfrage haben der Datenkontrolleur und/oder die Datenverarbeiter auf die Richtlinie hinzuweisen und die Daten fristgemäß und in Übereinstimmung mit den Bestimmungen der DSGVO zu entfernen.

Die Daten des Karteninhabers können vom Endbenutzer manuell aus dem ACT Enterprise-System gelöscht werden. Im System werden die verknüpften Protokollereignis-Daten dabei standardmäßig nicht gelöscht. Es gibt jedoch eine Einstellung zur Änderung dieser Voreinstellung, so dass die Protokollereignisse gelöschter Benutzer automatisch ebenfalls gelöscht werden.

## Wer hat Zugriff auf die Daten?

Der Datenkontrolleur und/oder Datenverarbeiter sind verpflichtet, offenzulegen, wer auf die auf dem am Standort installierten ACT Enterprise-System gespeicherten personenbezogenen Daten Zugriff hat. Der Datenkontrolleur und/oder Datenverarbeiter hat solche Verfahren zu erstellen und umzusetzen.

Enterprise verfügt über ein System an DB-Benutzern, die spezifischen Personen Rechte zur Kundensoftware gewähren können. Jeder Zugriff auf das System wird geprüft, u. a. Anmeldedaten, Änderungen an den Benutzerdaten und Vorgänge.

## Werden personenbezogene Daten außerhalb des EWR übertragen?

Im normalen Betriebsmodus werden die ACT Enterprise-Benutzerdaten nicht außerhalb des Systems weitergegeben. Es obliegt dem Datenkontrolleur und/oder Datenverarbeiter, offenzulegen, ob das System so konfiguriert ist, dass Daten außerhalb des EWR übertragen werden.