# Vanderbilt SMS

# EU General Data Protection Regulation – A Compliance Guide

## Contents

## Abstract

This guide is intended to help and support our customers in assessing their own readiness in meeting their responsibilities and obligations towards the new regulations.

## Overview

Data protection is a fundamental right whereby everyone has the right to the protection of personal data concerning him or her. The General Data Protection Regulation (GDPR) is applicable from 25th May 2018 and is designed to give individuals more control over their personal data. There is one set of rules for the whole of the EU, which can be complemented in some areas by national legislation.

The GDPR imposes obligations on businesses or organisations that collect, use and process personal data. At the centre of GDPR is the requirement for organisations and businesses to be fully transparent about how they are using and protecting personal data, and to be able to demonstrate accountability for their data processing activities. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

While Vanderbilt offers customers flexible and intuitive product functionality to facilitate compliance with the new regulations, the Vanderbilt organisation does not collect, control, use or process personal data which exists within Vanderbilt on-premises products. Therefore, it is the role and responsibility of the controller and processor of personal data to ensure that obligations stated in GDPR are complied with.

If you are in any doubt, or are unsure about the identity of the data controller and/or data processor in any case, you should consult your legal adviser.

## What is personal data?

The term “personal data” means any information relating to a living person who is identified or identifiable.

A person is identifiable if they can be identified directly or indirectly using an “identifier”. The GDPR gives examples of identifiers, including names, identification numbers, and location data. A person may also be identifiable by reference to factors which are specific to their identity, such as physical, genetic or cultural factors.

Personal data that has been de-identified, encrypted or pseudonymised but, can be used to re-identify a person remains personal data and falls within the scope of GDPR. If personal data has been rendered anonymous in such a way that the individual is no longer identifiable, then this is not considered personal data. For data to be truly anonymised, the anonymization must be irreversible.

The law protects personal data regardless of the technology or method used for processing that data – it applies to both automated and manual processing. It also doesn’t matter how the personal data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR.

## What constitutes data processing?

Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

The General Data Protection Regulation (GDPR) applies to the processing of personal data wholly or partly by automated means as well as to non-automated processing, if it is part of a structured filing system.

## Am I a data controller or data processer?

A data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files. Being a data controller carries with it legal responsibilities, so you should be quite clear if these responsibilities apply to you or your organisation.

If you or your organisation controls and is responsible for the personal data which it holds i.e. decides what personal information is going to be kept and to which use the information will be put, then you or your organisation is a data controller.

Examples of cases where the data controller is an individual include general practitioners, pharmacists, politicians and sole traders, where these individuals keep personal information about their patients, clients, constituents etc.

If you or your organisation holds the personal data, but some other individual or organisation decides and is responsible for what happens to the data, then that other individual or organisation is the data controller, and you or your organisation is a "data processor".

Examples of data processors include payroll companies, accountants and market research companies, all of which could hold or process personal information on behalf of someone else.

## What is data consent and do I need to consider it?

In order to legally process personal data, organisations and businesses must identify and document the legal basis for doing so from the start. Some of the legal ways to process data include:

- Consent of the individual: Consent is appropriate if individuals are offered real choice and control over how their data is used.
- Vital interests: Processing is necessary to protect the vital interests of the individual, e.g. if it's necessary to protect someone's life.
- Compliance that has a legal obligation: Data can be processed if for example, it is required by EU law for a particular purpose.
- A contract with the individual: Processing is necessary for the performance of a contract with an individual, e.g. to supply goods or services that have been requested

If you are in any doubt, as to whether you have acquired sufficient consent to process personal data, you should consult your legal adviser.

## What is a data processing contract and do I need to consider it?

If you hold or process (enter, edit, maintain) personal data (data processor) on behalf of your customer (data controller) you will require a data processing contract. We would recommend obtaining legal advice to best ensure the contract addresses appropriate security and other data protection safeguards. As part we would advise customers to have a checklist regarding data handling and the handover of the security system.

## Know your role and responsibility

It is clear the law is changing to GDPR and this needs to be factored into security system planning. Areas need be identified and addressed that may cause compliance problems under the GDPR. Under GDPR individuals have the right to be given clear information relating to the use of their data.

The first practical step is to identify your role and responsibility with respect to GDPR. Are you a data controller or data processor or both? If you are in any doubt, or are unsure about the identity of the data controller and/or data processor in any case, you should consult your legal adviser.

The second step is to become accountable. Consider all the personal data you are handling when working with the security system and examine it under the following headings:

- What personal data is stored?
- What is the legal basis on which processing of personal data is based?
- Where is the data stored?
- How is the data protected?
- How long is the data retained?
- What is the policy for handling individual data access requests?
- What is the process if someone asks to be removed from the system?
- Who has access to the data?
- Is personal data transferred outside the EEA?

# SMS & GDPR

The following information outlines the Vanderbilt SMS v6.x system functionality in relation to GDPR compliancy.

## What personal data is stored?

The only required personal data for a cardholder record is Last Name and Encoded Badge ID, though additional data is likely collected. First Name, Middle Initial and Cardholder Image are optional. User definable fields may also be used for entering various personal data as defined by the end user (customer).

## What is the legal basis on which processing of personal data is based?

The legal basis on which the personal data is obtained and processed is defined by the end user's policies and procedures. As an aid to the approval process, certain 3rd party applications with sophisticated consent and compliance workflow processes can be integrated with the SMS system.

## Where is the data stored?

The data is entered and owned by end user and is stored locally in SQL database or on the end user network (i.e. virtual server), or in backups managed by the end user. Aside from the Encoded Badge ID, no other personal data is stored on the hardware/system controllers. Additionally, the system does not allow for duplicate encoded IDs.

## How is the data protected?

SMS client software with password protected login is required to access the database. Users cannot log in to the SQL server directly.

User access privileges can be assigned to define to a high level of granularity ensuring that access to personal data is role-specific. Audit reports can be run to show operator login details.

Vanderbilt does not have access to customer data unless given specific permission and remote access for technical support.

## How long is the data retained?

Data retention requirements are defined and managed by the end user.

The Database Maintenance Utility in SMS is used to backup the database and to archive history files. It will also perform a complete defrag and re-index of all SMS tables and a complete purge of all records that have been scheduled for deletion. These functions can be run manually or they can be scheduled to run automatically. The end user should configure system Database Maintenance and archive file retention settings to comply per their country's or GDPR requirements.

## What is the policy for handling individual data access requests?

There are pre-defined Cardholder, Access and Audit reports that can be run in SMS and printed and/or exported in CSV and various structured formats such as Excel and PDF.

## What is the process if someone asks to be removed from the system?

If a request is made it is the responsibility of the data controller and/or data processors to outline the policy and to remove the data in a timely manner in accordance with GDPR regulations.

Cardholder records with associated personal data can be 'deleted' (i.e. flagged for deletion / hidden) from the client software or via an integrated 3rd party application with immediate effect. Personal data will be fully deleted from log events in accordance with user-defined system maintenance settings for database backups and archiving.

## Who has access to the data?

These details are defined and driven as per the corporate policies specific to and set by each end user.

Data is defined and entered by the end user, however it can also be populated via a 3rd party integrated system if approved and implemented as agreed by end user.

User access privileges can be assigned to define to a high level of granularity ensuring that access to personal data is role-specific. Audit reports can be run to show operator login details.

SMS allows the deletion of cardholder personal data from the database with full system cleanup and maintenance performed as per user-defined schedule or manual issuance. The Database Maintenance Module maintains the number of backups specified to be retained. Data archives are managed completely by the end user once created from SMS.

## Is personal data transferred outside the EEA?

SMS systems are installed globally, and may utilize 3rd party integrations as required and implemented by each end user. Any transfer of data disclosures would be the responsibility of said parties, or as managed by the end user.