



Vanderbilt ACT Enterprise

EU General Data Protection Regulation – A Compliance Guide

Contents

Abstract.....	2
Overview.....	2
What is personal data?	2
What constitutes data processing?.....	3
Am I a data controller or data processor?	3
What is data consent and do I need to consider it?.....	3
What is a data processing contract and do I need to consider it?	4
Know your role and responsibility	4
ACT Enterprise & GDPR.....	5



Abstract

Vanderbilt solutions and products enable customers to manage and process personal data in such a way as to meet GDPR requirements. 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 processor?

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?



ACT Enterprise & GDPR

The following information outlines how the Vanderbilt ACT Enterprise system can be used to facilitate GDPR compliancy.

What personal data is stored?

No personal data is mandatory to be stored in order for the ACT Enterprise system to function properly.

Image, name, email address and phone number are pre-defined fields in the system, but user definable fields could be used for entering various personal data.

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

The entry of data and the maintaining of data is controlled by the data controller and data processor of the site. As such it is the responsibility of the data controller and/or data processor to ensure the legal basis for processing the personal data is obtained.

There are no explicit procedures built-in to the ACT Enterprise software for obtaining user consent or recording it.

Where is the data stored?

The data is stored in the ACT Enterprise database located at the server and in backups. There can be some personal data stored in the system controllers (names) but this can be switched off by the system owner.

How is the data protected?

To access the content of the ACT Enterprise database, the client software (ACT Manage, Monitor, or Install) is used. The login, the software is protected by password.

We do not encrypt personal data. The end-user may choose to enforce encryption themselves, at a database level (SQL Server or SQL Compact).

Vanderbilt staff have no access to the customer's system, unless granted to via remote login.

How long is the data retained?

In ACT Enterprise, the card holder data is retained for as long as the person requires a card. Card validity end dates can be defined, but it is for the system user to arrange for the deletion of card holder data when it expires. Vanderbilt offer a card expiry report for making this process easy.

We have a feature to purge log events older than a set period of months, which can be customised by the user. By default, events are held in perpetuity.

Upon deleting a card holder, the system does not, by default, delete their related log events. But this can be changed to delete the log events when deleting the user.

What is the policy for handling individual data access requests?

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

There are several reports available in ACT Enterprise for detailing the information held about an individual, such as recent log events, including a way to export that data to standard PDF reports or CSV files



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.

Card holder data can be manually deleted from the ACT Enterprise system by the end-user. The system does not, by default, delete associated log event data. But there is a setting that can change this default, so that the log events of deleted users are also deleted with them.

Who has access to the data?

It is the responsibility of the data controller and/or data processor to disclose who has access to the personal data on the ACT Enterprise system installed on site. The data controller and/or data processor is responsible for creating and enforcing these processes.

Enterprise has a system of DB Users for granting rights to the client software to specific people. All access to the system is audited, including logins, changes to user data, and actions.

Is personal data transferred outside the EEA?

In normal operational mode ACT Enterprise user data is not shared outside the system. It is the responsibility of the data controller and/or data processor to disclose if the system is configured in a way which transfers data outside the EEA.