Vanderbilt Granta

EU General Data Protection Regulation – A Compliance Guide

Contents

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 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?

Granta & GDPR

The following information outlines how the Vanderbilt Granta V5.3 system can be used to facilitate GDPR compliancy.

What personal data is stored?

Collection of personal data is not mandatory within Granta, although it does have the capacity to store some user-definable fields, which could be used to store 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 into the Granta SW for obtaining user consent, or recording it.

Where is the data stored?

Data is stored both at the PC, and at the Granta controllers. The PC holds all information relating to the system, with the controller only holding data such as card numbers and access permissions as unique identifiers. It is not possible to restore names and other “personal” data from a controller.

How is the data protected?

The Granta database is stored in a specified SQL server, where certain connection properties can be modified to aid in the security of the data, and restricting access. Some information contained within the SQL database is in plain text, however things like PINs and Passwords are encrypted. With it being an SQL database, it’s also protected by standard access restrictions applied via Microsoft.

How long is the data retained?

Granta cardholder data is retained for as long as a cardholder exists within the system. Although validity of that cardholder can be set to specific start and end dates.

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.

It is possible to filter the events held in the Granta system to see what individual data is held about a person, e.g. recent log events, or information relating to their individual record.

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.

As default, event information is kept for 90 days on the Granta system, unless specified otherwise. Audit logs are kept indefinitely unless specified otherwise, however this logging does have to be enabled in the first instance. When a cardholder is deleted their associated events are not deleted, however it is feasible to do this via an SQL Script in SQL Management Studio.

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 Granta system installed on site.

Granta has the capability of defining different user logins to the software. Each user can be configured to have the necessary level of s/w access. It is the responsibility of the system owner to define who has what s/w login level, and remove access when it is no longer needed.

Is personal data transferred outside the EEA?

In normal operational mode Granta user data is not shared outside the system. Vanderbilt has no access to personal data. It is the responsibility of the data controller and/or data processor to disclose if personal data has been transferred outside the EEA.