

Vanderbilt International Data Protection Policy – SPC Connect

Date 17/04/2018

Version 0.1

This Privacy Policy explains how Vanderbilt International GmbH and its subsidiaries ("Vanderbilt" or "we") collect, store, use, disclose, share and transfer your information.

PLEASE READ THIS PRIVACY STATEMENT CAREFULLY BEFORE USING THE ENTIRE WEBSITE, SOFTWARE AND SERVICES OF VANDERBILT (COLLECTIVELY, THE "VANDERBILT SERVICES"). BY USING VANDERBILT SERVICES, YOU AGREE TO THIS PRIVACY POLICY AND AGREE TO THE COLLECTION, STORAGE, USE, DISTRIBUTION, SHARING AND TRANSFER OF YOUR DATA ACCORDING TO THIS PRIVACY POLICY. WE MAY AMEND THIS PRIVACY POLICY AT ANY TIME, PROVIDED THAT CERTAIN PROVISIONS OF THIS PRIVACY POLICY ARE INCOMPLETE OR OBSOLETE AND THAT SUCH CHANGES ARE REASONABLE IN THEIR INTEREST. IF WE MAKE SIGNIFICANT CHANGES TO THIS PRIVACY STATEMENT, WE WILL PUBLISH THE NEW VERSION ON THE WEBSITE, WHICH WILL BECOME EFFECTIVE IMMEDIATELY.

Introduction

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of Vanderbilt International with regard to the product SPC Connect. This includes obligations in dealing with personal data, in order to ensure that the organisation complies with the requirements of the relevant legislation, namely the GDPR. <https://www.eugdpr.org/>

Rationale

Vanderbilt International must comply with the Data Protection principles set out in the relevant legislation. This Policy applies to all Personal Data collected, processed and stored by Vanderbilt International in relation to its service providers and clients in the course of its activities.

Scope

The policy covers both personal and sensitive personal data held in relation to data subjects. The policy applies equally to personal data held in manual and automated form.

All personal and sensitive Personal Data will be treated with equal care by Vanderbilt International. Both categories will be equally referred to as Personal Data in this policy, unless specifically stated otherwise.

This policy should be read in conjunction with the associated Data Subject Access Request procedure, the Data Retention and Destruction Policy, the Data Retention Periods List and the Data Loss Notification procedure.

Vanderbilt International as a Data Controller

In the course of its daily organisational activities, Vanderbilt International acquires, processes and stores personal data in relation to:

- Customers of Vanderbilt International
- Third party service providers engaged with Vanderbilt International

In accordance with the GDPR, this data must be acquired and managed fairly. Not all staff members will be expected to be experts in Data Protection legislation. However, Vanderbilt International is committed to ensuring that its staff have sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the Data Protection Officer is informed, in order to ensure that appropriate corrective action is taken.

Due to the nature of the services provided by Vanderbilt International, there is regular and active exchange of personal data between Vanderbilt International and its Data Subjects. In addition, Vanderbilt International exchanges personal data with Data Processors on the Data Subjects' behalf.

This is consistent with Vanderbilt International's obligations under the terms of its contract with its Data Processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a Vanderbilt International staff member is unsure whether such data can be disclosed.

In general terms, the staff member should consult with the Data Protection Officer to seek clarification.

Subject Access Requests

Any formal, written request by a Data Subject for a copy of their personal data (a Data Subject Access Request) will be referred, as soon as possible, to the Data Protection Officer, and will be processed as soon as possible in accordance with GDPR regulations.

It is intended that by complying with these guidelines, Vanderbilt International will adhere to best practice regarding the applicable Data Protection legislation.

Third-Party processors

In the course of its role as Data Controller, Vanderbilt International engages a number of Data Processors to process Personal Data on its behalf. In each case, a formal, written contract is in place with the Processor, outlining their obligations in relation to the Personal Data, the specific purpose or purposes for which they are engaged, and the understanding that they will process the data in compliance with the GDPR legislation.

These Data Processors include:

- Internal Vanderbilt Support staff
- Atos IT Solutions and Services AB

The Data Protection Principles

The following key principles are enshrined in the GDPR legislation and are fundamental to the Vanderbilt International's Data Protection policy.

In its capacity as Data Controller, Vanderbilt International ensures that all data shall:

1. ... be obtained and processed fairly and lawfully.

For data to be obtained fairly, the data subject will, at the time the data are being collected, be made aware of:

- The identity of the Data Controller Vanderbilt International
- The purpose(s) for which the data is being collected
- The person(s) to whom the data may be disclosed by the Data Controller
- Any other information that is necessary so that the processing may be fair.

Vanderbilt International will meet this obligation in the following way.

- Where possible, the informed consent of the Data Subject will be sought before their data is processed;
- Where it is not possible to seek consent, Vanderbilt International will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- Where Vanderbilt International intends to record activity on CCTV or video, a Fair Processing Notice will be posted in full view;
- Processing of the personal data will be carried out only as part of Vanderbilt International lawful activities, and Vanderbilt International will safeguard the rights and freedoms of the Data Subject;
- The Data Subject's data will not be disclosed to a third party other than to a party contracted to Vanderbilt International and operating on its behalf.

2. be obtained only for one or more specified, legitimate purposes.

Vanderbilt International will obtain data for purposes which are specific, lawful and clearly stated. A Data Subject will have the right to question the purpose(s) for which Vanderbilt International holds their data, and Vanderbilt International will be able to clearly state that purpose or purposes.

3. not be further processed in a manner incompatible with the specified purpose(s).

Any use of the data by Vanderbilt International will be compatible with the purposes for which the data was acquired.

4. be kept safe and secure.

Vanderbilt International will employ high standards of security in order to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by Vanderbilt International in its capacity as Data Controller.

Access to and management of staff and customer records is limited to those staff members who have appropriate authorisation and password access.

5. ... be kept accurate, complete and up-to-date where necessary.

Vanderbilt International will:

- ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;

- conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date. Vanderbilt International conducts a review of sample data every six months to ensure accuracy; Staff contact details and details on next-of-kin are reviewed and updated every two years.
- conduct regular assessments in order to establish the need to keep certain Personal Data.

6. ... be adequate, relevant and not excessive in relation to the purpose(s) for which the data were collected and processed.

Vanderbilt International will ensure that the data it processes in relation to Data Subjects are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

7. ... not be kept for longer than is necessary to satisfy the specified purpose(s).

Vanderbilt International has identified an extensive matrix of data categories, with reference to the appropriate data retention period for each category. The matrix applies to data in both a manual and automated format.

Once the respective retention period has elapsed, Vanderbilt International undertakes to destroy, erase or otherwise put this data beyond use.

8. ... be managed and stored in such a manner that, in the event a Data Subject submits a valid Subject Access Request seeking a copy of their Personal Data, this data can be readily retrieved and provided to them.

Vanderbilt International has implemented a Subject Access Request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

Data Subject Access Requests

As part of the day-to-day operation of the organisation, Vanderbilt International's staff engage in active and regular exchanges of information with Data Subjects. Where a formal request is submitted by a Data Subject in relation to the data held by Vanderbilt International, such a request gives rise to access rights in favour of the Data Subject.

There are specific time-lines within which Vanderbilt International must respond to the Data Subject, depending on the nature and extent of the request. These are outlined in the Data Subject Access Request process.

Vanderbilt International's staff will ensure that, where necessary, such requests are forwarded to the Data Protection Officer in a timely manner, and they are processed as quickly and efficiently as possible, according to GDPR.

Implementation

As a Data Controller, Vanderbilt International ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation.

Failure of a Data Processor to manage Vanderbilt International's data in a compliant manner will be viewed as a breach of contract, and will be pursued through the courts.

Failure of Vanderbilt International's staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

Changes to This Privacy Policy

If we make material changes to our privacy policy that may impact you, we will prominently post notice of the change on our website within a reasonable period prior to the change becoming effective. We recommend that you check the Privacy Policy frequently so that you are informed of any changes.

What kinds of information do we collect?

Users of SPC Connect need to enter the following mandatory information during the registration process:

- Username
- Password
- First and Last Name
- Email
- Language
- Security Question information

In addition to the above the following optional fields may also be added by the user during the registration process.

- Other Names
- Address
- Post Code
- Phone Number

During the operation of SPC Connect the following information may also be linked to your account.

- Mobile Phone Identifiers (for Push Notification)
- Installation company information
- Access control information (User Image, card information, PIN, user rights)
- Alarm verification data (audio and /or video information)
- Audit Information

How do we use this information?

We use the information collected to provide a secure interface to your SPC systems, your information is also used by your installation company in order to offer services and to support you.

Where and how is my information stored?

Your information is stored within the EU and will not be transferred outside the EU. All SPC Connect information data is hosted on a database. Backups of the database happen regularly. Personal data is not replicated on any other system or used for any other purpose. The database access is strictly password protected. Only software engineers within Vanderbilt with the absolute need to access the database are allowed to do so. All access is strictly for management and control of the system, or for necessary debugging purposes.

How long is my data stored?

All information is saved for as long as the user leaves their account active on SPC Connect. The user can delete their account at any time. Once they delete their account all user information is deleted, however related information may link to the 'deleted' user – e.g. in Audit logs. Only the username will be used to link this information. If an SPC user account is not accessed within a 2 year period the account owner will be contacted, if the account owner does not access their account after the notice period the account will be deleted.

How is my data protected?

The database access is strictly password protected. Only software engineers within Vanderbilt with the absolute need to access the database are allowed to do so. All access is strictly for management and control of the system, or for necessary debugging purposes.

How is this information obtained?

SPC Connect users enter data manually through the web interface.

Legal basis on which processing of personal data is based?

Users accept the “terms and conditions” and “data protection policy” of the SPC Connect account on registration and the ability to delete their personal data exists within the application.

When using certain services within SPC Connect, “installer” users may enter information about “end users” without their explicit consent. In this use case it is the responsibility of the “installer” user to obtain consent from the “end user” and to manage this data.

How can I manage, delete or rectify information about me?

A user can manage, delete or rectify their account at any time within the SPC Connect application. The information is deleted as detailed above. If user wish to query or delete their data they must complete the form located at <https://www.spcsupportinfo.com/SPCConnectPro/forms/connect-query/>

How to I request access to my data

If user wish to query or delete their data they must complete the form located at <https://www.spcsupportinfo.com/SPCConnectPro/forms/connect-query/>

Children's Privacy Policy

Vanderbilt does not intend that any part of its Vanderbilt services will be used by children under the age of 16 or an equivalent minimum age in their jurisdiction, and such use is prohibited. If we actually learn that an account is connected to a registered user younger than 16 years of age, or an equivalent minimum age in the respective jurisdiction, we will immediately delete the information associated with that account. If you are a parent or guardian of a child under the age of 16 or an equivalent minimum age in your jurisdiction and believe that, he or she has provided us with personal information, please contact us by phone or email at the appropriate Vanderbilt Support Information for your country. A parent or guardian of a child under the age of 16 or an equivalent

minimum age in any jurisdiction may review and request the deletion of that child's personal information and prohibit its use

Global Activities

You consent to our information practices, including the collection, storage, use, processing and disclosure of your data as described in this Privacy Policy and the transfer and processing of your data to countries worldwide where we have or use facilities, service providers or partners, regardless of where you use our services. You acknowledge that the laws, regulations and standards of the country in which your information is stored or processed may differ from those of your country. In the European Economic Area (EEA) we store and store your personal data within the EEA in encrypted form, even if we use the data stored by third parties. We will not transfer them outside the EEA.

Contact Information

To ask questions or comment about this Privacy Policy and our privacy practices, please contact at <https://www.spcsupportinfo.com/SPCConnectPro/forms/connect-query/>

Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this Policy.

Data	This includes both automated and manual data. Automated data means data held on computer, or stored with the intention that it is processed on computer. Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Personal Data	Information which relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of the Data Controller. (If in doubt, Vanderbilt International refers to the definition issued by the Article 29 Working Party, and updated from time to time.)
Sensitive Personal Data	A particular category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, Information relating to mental or physical health, information in relation to one's Sexual Orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence.
Data Controller	A person or entity who, either alone or with others, controls the content and use of Personal Data by determining the purposes and means by which that Personal Data is processed.
Data Subject	A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.
Data Processor	A person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract, but who is not an employee of the Data Controller, processing such Data in the course of his/her employment.
Data Protection Officer	A person appointed by Vanderbilt International to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients
Relevant Filing System	Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.
