



Vretta

# DATA MANAGEMENT FRAMEWORK

This document describes the data management framework of policies followed at Vretta to comply with the European Union General Data Protection Regulation.

# Contents

<b>Overview .....</b>	<b>3</b>
The General Data Protection Regulation .....	3
<b>Roles and Responsibilities .....</b>	<b>4</b>
Data Controller and Data Processor .....	4
Sub-Processors .....	5
Data Protection Officer .....	5
Data Personnel .....	5
Agreements .....	5
<b>Data Policy .....</b>	<b>6</b>
General Policies.....	6
Data Storage.....	6
Electronic Form .....	7
Paper Form.....	7
Data Use.....	7
Data Accuracy .....	7
User Requests .....	7
Individual or Data Controller Request .....	7
Assisting the Data Controller .....	8
Data Breach Reporting .....	8
End of Service .....	8
Requests from Law Enforcement .....	8
<b>Ensuring Data Security.....</b>	<b>9</b>
Processing Activities .....	9
Transfer of Data .....	9
Redundancy and Back-Up Capabilities .....	10
Encryption of Personal Data.....	10
Ongoing Reviews of Security Measures.....	10
<b>Providing Information to the Public.....</b>	<b>10</b>
<b>Glossary .....</b>	<b>11</b>
<b>References .....</b>	<b>12</b>



## OVERVIEW

Vretta Inc. (also referred to as ‘Vretta’ or ‘company’ in this document) considers data security to be our top priority and are committed to maintaining the highest security standards in accordance with established best practices and legal requirements.

The company processes data for the purposes of reporting, tracking, monitoring etc. of the activity of individuals (also referred to as users) on their education technology platforms. The individuals can include students, teachers, government employees, and authorized employees and contractors at Vretta. We strive to manage user-data in a secure manner while helping them attain their educational goals.

This data management framework document serves to describe the processes and policies that have been established at Vretta to enable us to comply with the General Data Protection Regulation (GDPR). The policies described throughout this document will protect all parties from liabilities and harm by ensuring that Vretta complies with the regulations.

This data management framework applies to all offices and branches of Vretta, all staff and volunteers of Vretta and all contractors, suppliers, and other people working on behalf of Vretta. It applies to all data that the company holds relating to identifiable individuals.









## The General Data Protection Regulation

On May 25, 2018, the General Data Protection Regulation will go into effect. These regulations expand and strengthen the rights of individuals living in the European Union and provide new challenges to companies working within the EU.

The new regulations in the GDPR enhance the protection of personal data (any information that can identify a person, from names and emails to identification numbers). Personal data of a more sensitive nature (such as ethnicity or sexual orientation) is given even higher protection in the GDPR and requires stronger grounds to collect.

The GDPR applies to any organization that collects personal data from an individual residing in the European Union. This means individual rights are protected no matter where the organization is located. The right of consent has also been strengthened. In order to acquire personal information, consent must be an active process, separate from other processing, involving clear and plain language.

The GDPR establishes several principles that guide the philosophy and details of the regulation. They state that data must:

-  be processed fairly and lawfully,
-  be obtained only for specific, lawful purposes,
-  be adequate, relevant, and not excessive,
-  be accurate and kept up-to-date,
-  not be held for any longer than necessary,
-  be processed in accordance with the rights of data subjects,

- be protected in appropriate ways, and not be transferred outside the EU, unless that country or territory also ensures a comparable level of protection as per the General Data Protection Regulation (GDPR).

The GDPR provides the following new rights that enhance those previously provided by the Data Protection Directive:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The right not to be subject to automated decision-making including profiling



## ROLES AND RESPONSIBILITIES



### Data Controller and Data Processor

The GDPR distinguishes two important roles that classify what a company must do to comply with the regulation: Data Controller and Data Processor.

Vretta's clients and partners decide the purpose and method of data processing and are therefore considered Data Controllers. Vretta is considered a Data Processor since we process the data on behalf of the Data Controller, as per their instructions.

The key responsibilities of Vretta, as Data Processor are as follows:

- Maintaining record of processing activities, including,
  - details of the Data Protection Officer, Data Controller, Data Processor and any data representative,
  - categories of processing activities,
  - cross-border data transfers, and the
  - description of security measures implemented with respect to processed data.
- Ensuring data security, including,
  - encryption of personal data,
  - regular reviews of security measures, and
  - redundancy and back-up facilities.
- Placing confidentiality obligations on anyone processing personal/sensitive data.
- Ensuring Sub-Processors adhere to the GDPR.
- Aiding the Data Controller in demonstrating compliance (providing any information needed).
- Assisting the Data Controller in obtaining approval from Data Protection Authorities, if required.
- Reporting any data breaches to the Data Controller without undue delay.
- Review and maintain employee access to data






## Sub-Processors

Vretta uses tools and services from other companies for the purpose of project planning, project management, task management, quality control, communication, etc. These include cloud-based platforms or software. The companies that provide these services are considered Sub-Processors as they participate indirectly in our data processing function.

As the Data Processor, Vretta only uses services of Sub-Processors who are in compliance with the GDPR. As well, Vretta only uses Sub-Processors when we have prior written consent or a general authorization from the Data Controller. Vretta's Data Controllers are kept fully informed of any changes to our Sub-Processor use (see appendix).

## Data Protection Officer

Vretta's Data Protection Officer (DPO) oversees Vretta's compliance with the GDPR. Our DPO is an independent advisor who informs our employees on the obligations to the GDPR. The following list outlines the tasks of our DPO:

-  Oversee compliance with the GDPR.
-  Inform management personnel and employees of their obligations.
-  Train staff involved in processing activities.
-  Report to the highest level of management.
-  Be responsible for handling requests from individuals regarding their personal data and rights.

## Data Personnel

All personnel and contractors employed at Vretta have the responsibility for ensuring that any data that is collected is stored and handled appropriately in accordance with the Data Management Framework. Ultimately Vretta's management personnel is responsible for ensuring that Vretta meets its legal obligations.

## Agreements

Vretta considers data as highly confidential information and every entity (Vretta's Data Controller, Data Sub-Processor, Data Protection Officer, or Data Personnel) is bound by non-disclosure agreements (NDA).

Data Controllers have signed Contracts of Agreement that include a non-disclosure agreement. Data Personnel have signed Employment Contracts that include a non-disclosure agreement. Agreements with Sub-Processors are contained in the Terms and Conditions or Terms of Service of that company. More information on each Sub-Processor is included in the Appendix.









## DATA POLICY

Vretta has established policy protocols that describe both generally and in specific detail how the company adheres to the principles of the GDPR.



### General Policies

Only authorized employees can access data covered by this framework, to complete their tasks and obligations.

-  If employees are unsure about any aspect of data protection or may be concerned an action may violate a policy, they request help from their manager or the Data Protection Officer.
-  Vretta provides training to its employees to help them understand their responsibilities when handling data.
-  Data is regularly reviewed and updated if it is found to be out-of-date. If no longer required, it is permanently deleted.
-  Data is not shared informally. When access to confidential information is required, employees request it from their managers.
-  Personal data is not disclosed to unauthorized individuals, either within the company or externally.
-  Employees keep all data secure, by taking due care and following the more specific protocols and guidelines as follows.








### Data Storage

These rules describe how and where data is stored in accordance with the regulation.

#### Electronic Form

When data is stored electronically, it is protected from unauthorized access, accidental deletion, and malicious hacking attempts:





-  If data is stored on removable media/external storage, these are kept locked away securely when not being used, and only accessible with access credentials.
-  Data is backed up daily, overseen by the Technology Director. Those backups are tested regularly, in line with the company's standard backup procedures.
-  All servers and computers containing data are protected by VPC firewall as per the directives of the Technology Director.
-  Passwords for any storage medium or Sub-Processor are changed regularly.
-  All data is monitored in real-time, providing notification of unusual activity.

#### Paper Form

When data is received in printed format, it is stored in a secure place that is inaccessible by unauthorized personnel. These paper copies are shredded as soon as the intended purpose of processing has been achieved.





## Data Use

Data is not used by Vretta unless the company can use it for purposes specified by the Data Controller. However, it is when data is accessed and used that it can be at the greatest risk of loss, corruption, or theft:

-  Employees ensure their computers are always locked when left unattended.
-  Data is not shared informally.
-  Data at rest is protected by the firewall that protects our virtual private cloud.
-  Data is never transferred outside of the EU except to countries deemed appropriate by an Adequacy Decision from the European Commission.







## Data Accuracy

The law requires that Vretta takes reasonable steps to ensure data is kept accurate and up-to-date. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up-to-date.

-  Data is only held in as many locations as is necessary (including redundancy facilities).
-  Our staff takes every opportunity to ensure data is updated. We only reply to individuals from an approved contact list.
-  Vretta makes it easy for users to update the information Vretta holds about them.
-  Upon discovery of inaccuracies, data is updated.

## User Requests

All individuals who are the subject of personal data held by Vretta are entitled to:

-  ask what information the company holds about them and why,
-  ask how to gain access to it,
-  be informed how to keep it up-to-date,
-  be informed how the company is meeting its data protection obligations,
-  ask to delete it, and
-  ask us to transfer it, within feasible technical constraints, to another IT environment.

The GDPR states that the Data Controller is the primary point of contact and therefore responsible for handling user requests. In order to exercise their rights, an individual will contact the Data Controller to initiate the request, even if such data lives on servers belonging to the Data Processor. The Data Controller would then engage with the Data Processor in order to action their request accordingly. Under the GDPR, individuals can bring claims directly to Data Processors, however the Data Controller must verify the identity of anyone making an access request before handing over any information.

### Individual or Data Controller Request

All requests must be approved and validated through the Data Controller. In all situations, Vretta will be ready to use the following as a basic guide:

1. identify the individual with specific instructions from the Data Controller, and
2. identify and locate all data associated with that individual.

When there is a request based on the right of portability, Vretta will:

1. provide desired personal data in a machine-readable format (CSV).

When there is a request based on the right of erasure, Vretta will:

1. delete any relevant data from database, and
2. delete any other references from any sources as located on Personal Data Inventory.

When there is a request based on the right of rectification, Vretta will:

1. identify the source of the error,
2. identify a way to correct the error, and
3. correct the error.



## Assisting the Data Controller

To aid the Data Controller in demonstrating compliance, Vretta will provide any information needed to the Data Controller as per its contract of agreement while adhering to the regulations. As well, Vretta will provide information to assist the Data Controller in obtaining approval from Data Protection Authorities if it is required.



## Data Breach Reporting

In order to identify breaches, Vretta has real-time monitoring to track unusual activity. If, in the event of loss of integrity, confidentiality, or availability, Vretta will take appropriate measures to minimize risk. If the breach is likely to pose a risk to an individual's rights and freedoms, Vretta will notify the Data Controller without undue delay. Every breach will be reported to the Data Controller.



## End of Service

Excepting any specific agreements, at the end of our relationship with any Data Controller we will delete or return all personal data as per their instructions and contract of agreement.



## Requests from Law Enforcement

In certain circumstances, data may be required to be disclosed to law enforcement agencies without the consent of the user (such as a legal subpoena). Under these circumstances, Vretta will keep the Data Controller informed of the request to the fullest extent as permitted by the law. The Data Controller will ensure the request is legitimate, seeking assistance from the management personnel and from the company's legal advisers, where necessary. If the request is legitimate, Vretta will be required to disclose the requested data to the law enforcement agencies.





## ENSURING DATA SECURITY

The following section describes more technical aspects of Vretta's data security policy.



### Processing Activities

A cornerstone of the GDPR is organizational accountability. To achieve this, Vretta maintains records of all its processing activity. We keep documentation with a specific record of the categories of data processing, including,

- 🔒 collecting,
- 🔒 storing,
- 🔒 accessing,
- 🔒 modifying,
- 🔒 dissemination and
- 🔒 deletion of data.

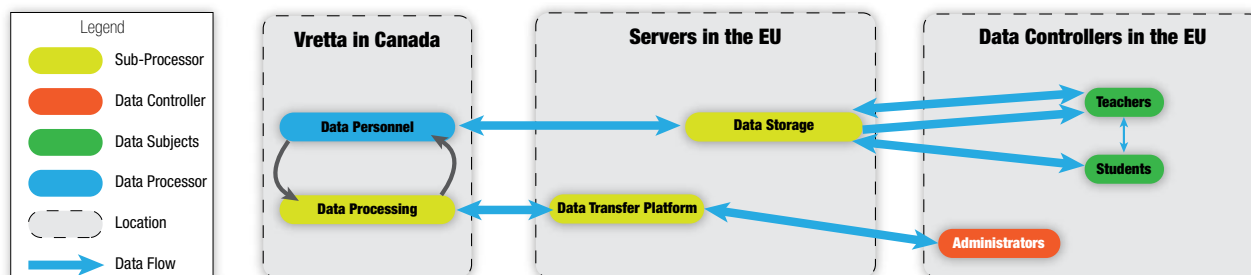


### Transfer of Data

Data from the use of Vretta's products is only transferred within countries that have adequate regulations. This is limited to the members of the European Union and other countries accepted by an "Adequacy Decision" by the European Commission, such as Canada.

The data transfer process starts in the country where the product is being used by students and teachers (users). When users access the platform, data is directed to servers in Europe which log and store the data. Data on these servers is then transferred to Canada (Vretta office) where it is processed by authorized data personnel. Once this processing is complete, Vretta sends the data back to Europe, where it is stored and accessible to our clients. Based on the application of the product, Vretta has customized data transfer flowcharts that are provided to the respective Data Controllers.

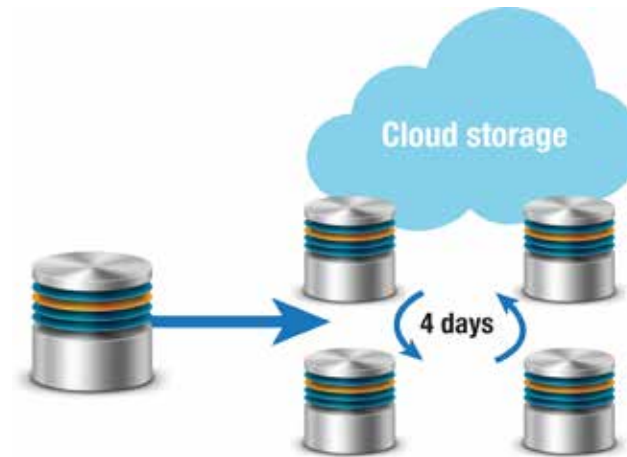
At the end of this transfer process, data is stored using an approved Sub-Processor that the Data Controller can access. The accounts for these Sub-Processors are password protected. Administrators have access to this storage using passwords provided by Vretta.



*Note: Transfer process may vary based on the product and the agreement with the Data Controller.*

## Redundancy and Back-Up Capabilities

Vretta has put in place redundancy and back-up capabilities physically located in the European Union. Every night, a snapshot of the data is created and stored on a set of different server images on the cloud. This image of the data is kept for the next 4 days. This means that we have, at any given time, 4 distinct snapshots of all our data.



## Encryption of Personal Data

Data in transit is encrypted to maintain the specific configuration necessary to achieve 'A' grade on the Qualys SSL Labs report. Our cipher strength, key exchange, protocol support and certificate are all rated highly. Data at rest is protected by the firewall that protects our virtual private cloud.

## Ongoing Reviews of Security Measures

Internal reviews of security measures take place monthly to assess the standards of any security measures in place concerning personal and sensitive data. Management personnel is informed of the quality of the data security and any improvements needed are made.



## PROVIDING INFORMATION TO THE PUBLIC

Vretta aims to ensure that individuals using our technology platforms are aware that their data is being processed and that they understand how the data is being used. This enables them to exercise their rights. The company has a [Privacy Statement](#), setting out how data relating to individuals is used by the company. Vretta also has a section on [Data Protection](#), summarizing its adherence to the GDPR.



## GLOSSARY

The following terms are used in this Data Management Framework document and defined in the context and for the purposes of the GDPR.

**Adequacy Decision** When the European commission has decided a country has adequate protections, equivalent to those of the GDPR.

**Cross-Border Transfers** Any exchange or movement of data from one country to another.

**Database** A structured collection of tables holding data in several formats, accessible through queries.

**Data Breach** An event with the loss of integrity, accuracy, confidentiality of personal data.

**Data Controller** A Data Controller is an entity that decides the purpose and method of processing personal data.

**Data Processor** A Data Processor is an entity that holds, stores, uses, analyzes, deletes, transmits, disseminates, or collects personal data.

**Data Protection Directive** Directive 95/46/EC was adopted in 1995 and established rights which would be enhanced and expanded in the GDPR.

**Data Protection Officer** The Data Protection Officer (DPO) is required under certain circumstances. These include when the Data Controller or data processor is monitoring personal data on a regular basis, on a large scale. The DPO will oversee the organization's activities and ensure it complies with GDPR.

**Data Storage** Any method of archiving data in electronic or paper form. Database management systems (DBMS) are typically used.

**Data Sub-Processor** A Data Sub-Processor performs processing operations on behalf of the Data Processor.

**General Data Protection Regulation** This law enhances and expands on the rights of the Data Protection Directive from 1995. Included are new obligations for Data Controllers and Data Processors, stronger requirements for consent, and the expansion of its territorial scope from Europe to any organization working with personal data from European residents.

**Personal Data** Any information which can, directly or indirectly, identify a person or user through the use of a name, identification number, location, or any physical, mental, economic, or social characteristics.

**Public Administration** An organization at the national, regional, or local level which is considered a public authority in a particular country or state.

**Redundancy and Back-Up Facilities** Methods of ensuring data availability, protecting against failure, and having separate copies of data in multiple places.

**Sensitive Data** A sub-category of Personal Data, sensitive data covers information relating to ethnicity, race, sexual orientation, health, religious or philosophical beliefs, political opinions, and genetic and biometric data.



## REFERENCES

Are you ready for the new data protection rules? 10 questions to help prepare your organization for the General Data Protection Regulation (GDPR) [PDF file]. (n.d.).

<https://cnpd.public.lu/content/dam/cnpd/en/dossiers-thematiques/Reglement-general-sur-la-protection-des-donnees/Reglement-general-sur-la-protection-des-donnees/CNPD-10-questions-EN-web.pdf>.

GDPR Key Changes. An overview of the main changes under GDPR and how they differ from the previous directive. (n.d.).

*Retrieved from:* <https://www.eugdpr.org/key-changes.html>.

General Data Protection Regulation: a guide to assist processors. (2017, November 27).

*Retrieved from:* <https://www.cnil.fr/en/general-data-protection-regulation-guide-assist-processors>.

Guide to the General Data Protection Regulation (GDPR). (n.d.).

*Retrieved from:* <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>.

Rights and obligations. (2015, December 29).

*Retrieved from:* <https://www.cnil.fr/en/rights-and-obligations>.

Rules for business and organizations. Find out what your organization must do to comply with EU data protection rules and learn how you can help citizens exercising their rights under the regulation. (n.d.).

*Retrieved from:* [https://ec.europa.eu/info/law/law-topic/data-protection/reform\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform_en).

What is personal data? (n.d.).

*Retrieved from:* [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en).

What is a data controller or a data processor? (n.d.).

*Retrieved from:* [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en).

What are the responsibilities of a Data Protection Officer (DPO)? (n.d.).

*Retrieved from:* [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/data-protection-officers/what-are-responsibilities-data-protection-officer-dpo\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/data-protection-officers/what-are-responsibilities-data-protection-officer-dpo_en).



[www.vretta.com](http://www.vretta.com)

[info@vretta.com](mailto:info@vretta.com) | [legal@vretta.com](mailto:legal@vretta.com)

**CANADA**  
120 Adelaide Street East  
Toronto, ON M5C 1K9

**LUXEMBOURG**  
6, rue Tubis  
L-2629 Luxembourg

**UNITED KINGDOM**  
20-22 Wenlock Road  
London N1 7GU