



Privacy and Personal Data Protection Policy

DOCUMENT CLASSIFICATION	Public
DOCUMENT REF	ISMS-DOC-A05-34-1
VERSION	1.2
DATED	21 July 2025
DOCUMENT AUTHOR	Gabriela Murillo, Cybersecurity and Compliance Team Leader
DOCUMENT OWNER	Erick Valverde, CIO, VP of Information Systems and Security

Privacy and Personal Data Protection Policy
Public

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1	09/11/2023	-	Initial version.
1.1	07/09/2025	Gabriela Murillo	Updated the section "Notice to residents of countries outside of the United States of America". Added DPF and GDPR principles to the policy.
1.2	07/21/2025	Gabriela Murillo	Aligned the whole content to DPF.

Distribution

NAME	TITLE

Approval

NAME	POSITION	SIGNATURE	DATE
Erick Valverde	CIO, VP of Information Systems and Security		

Contents

1	Introduction.....	4
2	Privacy and personal data protection policy	5
2.1	The General Data Protection Regulation	5
2.2	Definitions	5
2.3	Principles relating to processing of personal data	5
2.4	Privacy by design	6
2.5	Data Protection Officer	7
2.6	Breach notification.....	7
2.7	EU-U.S., UK-U.S. Data Privacy Framework Compliance	7
2.7.1	DPF commitment	9
2.7.2	U.S. entities or subsidiaries adherence.....	9
2.7.3	FTC investigatory and enforcement powers.....	9
2.7.4	Binding arbitration	9
2.7.5	Third party disclosures.....	9
2.7.6	Liability for onward transfers.....	10
3	Contact us.....	10

1 Introduction

In its everyday business operations VerusRx, LLC makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees
- Customers
- Users of its websites
- Subscribers
- Other stakeholders

In collecting and using this data, the organization is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps VerusRx is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to VerusRx's systems.

The following policies and procedures are relevant to this document:

- *Information Classification Procedure*
- *Information Labelling Procedure*
- *Records Retention and Protection Policy*
- *Acceptable Use policy*
- *Internet Acceptable Use Policy*
- *Information Security Incident Response Procedure*
- *Information Security Roles, Responsibilities and Authorities*

2 Privacy and personal data protection policy

2.1 The General Data Protection Regulation

The General Data Protection Regulation 2016 (GDPR) is one of the most significant pieces of legislation affecting the way that VerusRx carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of citizens of the European Union. It is VerusRx's policy to ensure that our compliance with the GDPR and other relevant legislation is clear and demonstrable at all times.

2.2 Definitions

There are a total of 26 definitions listed within Article 4 – Definitions of the GDPR and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:

Personal data is defined as: *“any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”*

Processing means: *“any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as 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.”*

Controller means: *“the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.”*

2.3 Principles relating to processing of personal data

There are several fundamental principles upon which the GDPR is based.

These dictate that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

Privacy and Personal Data Protection Policy
Public

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation').
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
4. Accurate and, where necessary, kept up to date ('accuracy')
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation').
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

In addition, the controller shall be responsible for, and be able to demonstrate compliance with all of these principles ('accountability').

VerusRx must ensure that it complies with all these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems. The operation of an information security management system (ISMS) that conforms to the ISO/IEC 27001 international standard is a key part of that commitment.

2.4 Privacy by design

VerusRx has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data will be subject to due consideration of privacy issues, including the completion of one or more privacy (also known as data protection) impact assessments.

The privacy impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization and pseudonymisation will be considered where applicable and appropriate.

2.5 Data Protection Officer

A defined role of Data Protection Officer (DPO) is required under the GDPR if an organization is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

Based on these criteria, VerusRx has appointed David Baker as the Data Protection Officer (DPO).

The DPO will be provided with the necessary resources to fulfill their tasks and maintain their expert knowledge of data protection law and practices. The DPO will operate independently and will not be dismissed or penalized for performing their tasks. They will report directly to the highest level of management.

The main tasks of the DPO include:

- Monitoring compliance with the GDPR and other data protection laws.
- Providing advice on data protection impact assessments (DPIAs).
- Cooperating and acting as a contact point for the supervisory authority.
- Advising on data protection obligations.

The contact details of the DPO will be provided to data subjects and the supervisory authority as required.

2.6 Breach notification

It is VerusRx's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. This will be managed in accordance with our *Information Security Incident Response Procedure* which sets out the overall process of handling information security incidents.

2.7 EU-U.S., UK-U.S. Data Privacy Framework Compliance

VerusRx is committed to complying with the principles of the EU-U.S. Data Privacy Framework and UK Extension to the EU-U.S. DPF. These frameworks enhance our ability to transfer personal data from the European Union and the United Kingdom to the United States while ensuring adequate protection and adherence to stringent data protection standards.

Privacy and Personal Data Protection Policy
Public

Principles of the DPF:

- **Notice:** We inform individuals about the purposes for which we collect and use their personal data, the types of third parties to which we disclose the data, and the means we offer individuals to limit the use and disclosure of their data.
- **Choice:** We offer individuals the opportunity to choose (opt-out) whether their personal data is to be disclosed to a third party or to be used for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual.
- **Accountability for Onward Transfer:** Prior to transferring personal data to a third party, we ensure that the third party adheres to the principles of the DPF or commits to provide adequate protections by contract.
- **Security:** We take reasonable and appropriate measures to protect personal data from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.
- **Data Integrity and Purpose Limitation:** We limit the collection of personal data to what is relevant for the purposes of processing and ensure that such data is reliable, accurate, complete, and current. We only process personal data in a way that is compatible with the purposes for which it has been collected or subsequently authorized by the individual.
- **Access:** We provide individuals with access to their personal data and allow them to correct, amend, or delete information where it is inaccurate or has been processed in violation of the principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy.
- **Recourse, Enforcement, and Liability:** We provide robust mechanisms for ensuring compliance with the DPF principles and resolving disputes about our adherence to these principles, including recourse through independent dispute resolution mechanisms.

Independent Recourse Mechanism for Non-HR Data: As part of our commitment under the DPF, VerusRx has designated the following independent recourse mechanism to address complaints and provide appropriate recourse free of charge to the individual:

- **For EU-U.S. DPF:** EU Data Protection Authorities (DPAs)
- **For UK-U.S. DPF:** UK Information Commissioner's Office (ICO).

This policy enhancement ensures clarity regarding our international data transfer mechanisms and our dedication to protecting the privacy and security of personal data under various legal frameworks, including the DPF.

2.7.1 DPF commitment

VerusRx complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, as set forth by the U.S. Department of Commerce. VerusRx has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>.

2.7.2 U.S. entities or subsidiaries adherence

VerusRx informs individuals that the following U.S. entities or U.S. subsidiaries also adhere to the EU-U.S. DPF Principles, including as applicable under the UK Extension to the EU-U.S. DPF and are covered by our organization's DPF submission.

- Verus RX, LLC
- Verus RX II, LLC

2.7.3 FTC investigatory and enforcement powers

VerusRx is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

2.7.4 Binding arbitration

Under certain conditions, individuals may invoke binding arbitration. VerusRx is obligated to arbitrate claims and follow the terms as set forth in Annex I of the DPF Principles, provided that an individual has invoked binding arbitration by delivering notice to us and following the procedures and subject to conditions set forth in Annex I of the Principles.

2.7.5 Third party disclosures

VerusRx may disclose personal information to the following types of third parties and for the following purposes:

- **Service Providers:** To provide, maintain, and improve our services. These service providers are required to adhere to the DPF Principles or provide adequate protections by contract.

Privacy and Personal Data Protection Policy
Public

- **Partners:** For joint marketing and research purposes, with the appropriate consent of individuals where required.
- **Legal Obligations:** To comply with legal obligations, such as responding to lawful requests by public authorities, including to meet national security or law enforcement requirements.

2.7.6 Liability for onward transfers

VerusRx acknowledges its liability in cases of onward transfers to third parties.

3 Contact us

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, VerusRx commits to resolve DPF Principles-related complaints about our collection and use of your personal information. EU and UK individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, should first contact VerusRx at:

David Baker

EVP & Chief Information Officer

VerusRx

12221 Merit Drive, Suite 1800
Dallas, TX 75251

Email: dbaker@nationalppo.com

Phone: (214) 269-9908