Verteda Limited

GDPR Product Statement

Verteda Ltd GDPR Product Statement

Contents

1. Overview 3
2. Personal and Sensitive Data – Statutory Definitions 4
3. The Eight Rights of The Act 6
   3.1 The Right to Be Informed 7
   3.2 The Right to Access 7
   3.3 The Right to Erasure 8
   3.4 The Right to Rectification 8
   3.5 The Right to Object 8
   3.6 The Right to Restrict Processing 8
   3.7 The Right to Portability 9
   3.8 The Right to Manual Processing 9
4. How the data is retained and removed 10
5. Consent Management 11
6. How the Data is Secured 11
7. Prerequisites 12

1. Overview

The purpose of this document is to give an overview of how the software products of Verteda Limited (Verteda) will assist customers with their compliance with the GDPR.

The document will cover the 8 rights of the individual within the act and how the products will aid with compliance in these areas.

This document will also provide examples of personal and sensitive data that Verteda may hold within standard fields in the system.

Wherever possible Verteda will provide the full ability for the client to self-service the amending, retrieval or removal of data as required by GDPR.

Within this document we will refer to the 'client' as being the Customer, or any person associated or an authenticated physical user of the Verteda solutions.

A major point that should be made is that GDPR and security compliancy is a shared responsibility between Verteda and its Customers which require separate obligations to be fulfilled.

Release versions as recommended by Verteda for GDPR compliancy will be a prerequisite (see Section 7 below) to Verteda accepting its joint Data Processor liability under GDPR.

2. Personal and Sensitive Data – Statutory Definitions and Privacy Impact Statements

2.1 Examples of personal data

Names	
Addresses	
Date of Birth	
National Insurance Number	
Gender	
Next-of-kin details	
Image	E.g.. digitalised photo of the user
Warnings	
Notes/Comments	Ad-hoc personal comments that may be entered
Forms	Customers need to consider non-standard fields stored in Forms created/customised by the client
Extra Client Fields	Customers need to consider sensitive data that may be stored in Extra Data fields created/customised by the client

2.2 Examples of Sensitive Data

Ethnic Origin	
Sexuality	
Religion	
Bank Account details	
Medical details	Communication preferences, impairments etc
Criminal history	
Social Work	
Eligibility to work details	Visas, passports
Notes/Comments	Ad-hoc personal comments that may be entered
Forms	Customers need to consider non-standard fields stored in Forms created/customised by the client
Extra Client Fields	Customers need to consider sensitive data that may be stored in Extra Data fields created/customised by the client

2.2 Customer's responsibilities

A Customer's Data Controller Statement should say why the data is captured, for what purposes and how long it is retained. This is to comply with the parts of the GDPR that state that data is collected lawfully, fairly and in a transparent manner. In reality, this will require each customer to perform a privacy impact assessment on personal and sensitive data that it collects and processes. There is guidance on the ICO website regarding performing privacy impact assessments. The statement must also show how the data is kept up to date and is accurate and is only held for the period where it is relevant. How the data is stored, secured and monitored for unauthorised access should also be detailed.

For personal data, the following legal gateways are valid.

- Consent
- Necessary in relation to the processing of a contract
- Legal obligation
- Vital interest – a matter of life and death
- Justice, Government, Statutory
- Legitimate interest

For sensitive data, the following are also valid.

- Consent
- Employment law
- Vital interest
- Legal proceedings, Legal advice or defending legal rights
- Administering justice
- Medical Reasons
- Equal opportunity monitoring with safeguards
- Crime prevention / malpractice

Verteda will carry out its own Privacy Impact Assessments (PIA) for all software and services supplied by Verteda under a Customer contract. However this will be generic to the software or services and not specific to the use to be made by the Customer of the personal data it captures using our software and services, as this is unique for each Customer. Therefore, in order to ensure that, as a Data Controller, the Customer has complied with its obligations under GDPR, each Customer will need to complete its own PIA.

Verteda can only warrant software release versions as recommended by Verteda for GDPR compliancy, and use of such GDPR compliant versions by the Customer will be a legal prerequisite (see Section 7 below) to Verteda accepting its liability under GDPR as Data Processor.

3 The Eight Rights of The Act

3.2 The Right to Be Informed

As a Data Controller, the Customer should inform the data subject of the types of data that it is capturing, why you are capturing it and how long it is retained. It is also necessary to inform the data subject regarding how data is shared with other systems and why.

Verteda Products and Services

- *Vantage*
- *QJacker*
- *Virtual Manager*
- *Primo*
- *Ticketing*
- *Gaming Interface*
- *Challenge 25*
- *Business Intelligence*
- *Interval Pre-Orders*
- *Events 500*
- *Infogenesis*
- *Eatec*
- *EMV Interface*
- *Voyager 1 & 2*

3.3 The Right to Access

To comply with the Subject Access Request element of the Regulation Verteda will provide the client with full access to the client's data through the solution. This may be as an individual self-service portal as a standard, or requested through the client's internal support mechanisms. The Verteda solutions have the ability for the customer to individually/group authorise the various areas of their solutions depending on their requirements. Where the Customer utilises central operations to provide the function to clients, then the Customer should create a Subject Access Report as a contact management record against the client with a defined set of actions and outcomes that allow reporting on the requests and their status. If self-service does not meet any of the requirements for the right to access for the client for any reason, then the Customer will need to raise a Subject Access Request (SAR) on the Verteda support system by the Customer's authorised personnel, for actioning by Verteda.

3.4 The Right to Erasure

Following on from a Subject Access Report a Customer may request all or partial erasure of data. The erasure request should be created as a contact management record against an individual with a defined set of actions and outcomes that allow reporting on the requests and their status. It is suggested that, before and after, a Subject Access Report is provided as proof of the removal along with a confirmation letter stating the outcome of the process. If self-service does not meet any of the requirements for the right to erasure for the data subject for any reason, then a Subject Access Erasure will be able to be raised on the Verteda support system by the Customer's authorised personnel, for actioning by Verteda.

3.5 The Right to Rectification

Following on from a Subject Access Report a client may request all or partial rectification of data. The rectification request should be created as a contact management record against the data subject with a defined set of actions and outcomes that allow reporting on the requests and their status. It is suggested that, before and after, a Subject Access Report is provided as proof of the rectification along with a confirmation letter stating the outcome of the process. If self-service does not meet any of the requirements for the right to rectification for the individual for any reason, then a Subject Access Rectification will be able to be raised on the Verteda support system by the Customer's authorised personnel, for actioning by Verteda.

3.6 The Right to Object

Following on from a Subject Access Report a data subject may object to certain aspects of processing. The request should be created as a contact management record against the individual with a defined set of actions and outcomes that allow reporting on the requests and their status.

It is suggested that the individual is sent a confirmation letter stating the outcome of the process.

3.7 The Right to Restrict Processing

Following on from a Subject Access Report a client may object to certain aspects of processing. The request should be created as a contact management record against the individual with a defined set of actions and outcomes that allow reporting on the requests and their status.

It is suggested that the individual is sent a confirmation letter stating the outcome of the process.

3.8 The Right to Portability

A data subject may request an export of their data in a recognisable format. The request should be created as a contact management record against the individual with a defined set of actions and outcomes that allow reporting on the requests and their status. It is suggested an export is provided of the data along with a confirmation letter stating the outcome of the process. If the data subject has requested erasure of their data, then a confirmation certificate should also be provided. If self-service does not meet any of the requirements for the right to portability for the client for any reason, then a Subject Access Portability (SAP) will be able to be raised on the Verteda support system by the Customer's authorised personnel, for actioning by Verteda.

3.9 The Right to Manual Processing

Following on from a Subject Access Report a data subject may request manual intervention in a process. The request should be created as a contact management record against the individual with a defined set of actions and outcomes that allow reporting on the requests and their status.

It is suggested that the data subject is provided with a confirmation letter stating the outcome of the process.

4 How the data is retained and removed

This section relates to the data minimisation by implementing a retention policy on key records and fields.

The aim of Data Archiving is to aid compliance with the Data Retention Polices as set out in GDPR.

Minimisation of all data accessible to users is provided as a facility (based on individual or group authorisation) to all Customers; it is the responsibility of the Customer to inform Verteda when permanent or hard deletion of inaccessible data is further required.

Verteda operates a 30 day data backup retention period only, save for database back up which is for a period of 12 months..

5 Consent Management

A new section of a data subject's personal records should be introduced where consent for processing can be managed. This will require new fields that describe the type of usage of the data, the type of data being processed, the legal gateway being used to justify the usage and the start and end period of the consent. Where restrictions or objections to processing are deemed appropriate to interfaces then the consent records should be checked to prevent export of any said data.

Verteda will assume that if a data subject is provided by the Customer with an authorised user logon details, that the data subject has provided consent to the usage and any data processing within the Verteda solutions.

6 How the Data is Secured

The Verteda software products implement the best practice with a layered and organised structure to provide Privacy by Design.

The Verteda Solutions and environments will provide for the best security and availability practices including:

- Tier 4 data-centres usage as a minimum to ensure constant availability of access to data;
- Firewalling controls;
- Anti-Virus/Malware services;
- IPS/IDS servicing;
- 24-hour systems' monitoring and alerting functions;
- obfuscation/encryption of any sensitive data; encryption of all traffic between systems, including to the Customer's system;
- authentication options for password controls and complexity;
- authorisation levels with no access by default and least required level access provision.

In addition, Verteda support personnel follow security training, policies and procedures, and additionally will not have direct access to view or extract client sensitive data direct from data sources.

7 Prerequisites to ensuring Compliancy

1. Verteda Software products which are compliant:

- *Vantage*
- *QJacker*
- *Primo*
- *Ticketing interface*
- *Gaming Interface*
- *Interval Pre-Orders*
- *Events 500*
- *Voyager 1 & 2*

(Third party products are the responsibility of the third party owner)

2. Customer is required to have a Verteda support and maintenance services contract in place.

Other Recommendations from Verteda:

Review of access to Verteda supplied software and services granted to staff/work groups.

Microsoft security updates are implemented on all machines.

Device security updates are implemented.

Anti-virus and malware software is implemented and up to date.

Device management software for mobile devices are implemented and up to date.

Customer should review any third-party software that they directly integrates with Verteda solutions and their use of them in relation to personal data.

Further reading:

UK Information Commissioner's Office(ICO): https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

EU Commission: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN