Vergic Data Protection Policy (VDPP)

Table of Contents

Document name and version: VDDP 1911
Rickard Janz 2018-05-02, revised 2019-11-07

1 ORGANISATION

Vergic has appointed a Data Protection Officer (DPO). All policies, activities such as implementation, information, training, risk assessment, security testing etc. described in this document falls under the responsibility of the DPO.

Appointed DPO is Stefan Möhl (Vergic CTO) who is also part of the management team. The Data protection policy (DPP) as a whole is decided upon as a Management decision.

1.1 Locations

With the possible exception of customers that reside outside of the EU all processing and storage of personal data takes place inside the European Union (Sweden).

1.2 Sub-contractors

Vergic data center facilities in Stockholm and Falkenberg, Sweden are operated by GleSYS. The data center facilities and operational staff controls physical access to Vergic servers.

Vergic has signed a back to back data processing agreement with GleSYS.

GleSYS staff are not able to read any data on the servers, the data is encrypted and GleSYS personnel does not have access to Vergic data in unencrypted format.

GleSYS/Vergic have agreed on a detailed quality and security management system for the facilities.

2 CATEGORIES OF PERSONAL DATA THAT ARE PROCESSED

2.1 Vergic Engage Standard

As standard, two types of personal data might be processed and stored;

1. IP-number – personal record by default
2. Chat Transcript – *might* contain personal data such as name and social security number in running text. This is not collected by default, but the customer might enter such data in running text while chatting

Since some Chat Transcripts will contain personal data Vergic standard policy is to treat all chat transcripts as if containing personal data.

2.2 Vergic Engage Custom Settings

Only if defined in the DPA with a customer, more types of personal data might be processed and stored;

Example of such data is:

3. E-mail address
4. Social security number
5. Customer ID

if integration exists with authentication service or with CRM/similar system the authentication key can also be processed and stored against the session

3 PROCESSING OF DATA

Vergic Engage is a cloud SAAS application. The system can be deployed as public or private cloud. For details see appendix: Vergic Cloud computing platform.pdf.

3.1 Pre-chat

As a web visitor enters a web page where Vergic Engage is implemented a profile is being created of all visitors which is then analysed through the engagement rules and proactive scoring algorithms.

1. Vergic Engage Standard – no personal data is collected on the profile (pre-chat)
2. IP-number is saved in the web activity logs for security reasons
3. Vergic Engage Custom settings – Only if defined in the DPA with a customer. Personal data, see 2.2 above (for instance CRM data) might be processed in order to determine who to engage with

3.2 During a chat

Personal data according to chapter 2 above can be processed. Vergic Engage can be configured to search for and automatically erase text (chat) input data in the form of regular expressions. From a personal data perspective this is typically represented by a social security number.

3.3 Safeguards for data transfer

All data is transferred under the https protocol.

VPN, security tokens and other measures can be added to further strengthen security if needed in integrations.

4 STORAGE OF PERSONAL DATA

The general principle from a personal data protection perspective has been pseudonymisation through encryption.

Production data bases as well as backups are encrypted through AES256, as well as by checksummed.

4.1 Production data bases

Vergic Engage is a cloud service with an industry strength application architecture. Vergic Engage is a highly scalable, redundant and secure SaaS platform. SaaS, scalability, security and redundancy systems are inherently complex and expensive. There are many moving parts that need to work together. The Vergic cloud computing is the workhorse for Vergic Engage.

See appendix: Vergic Cloud computing platform, for more details on system architecture and data bases.

4.1.1 Vergic Engage Standard & Vergic Engage Custom Settings

Data that is stored according to 2.1 above, for retention policy and periods see chapter 6.

1. IP-number is not stored in the application itself but can be connected to a chat session by Vergic support staff is needed. IP-addresses are stored in temporary web activity logs by a session key in the application logger tool.
2. Chat transcripts are stored in customer account data in the application databases. Chat transcripts can be retrieved by account users with necessary privileges. Vergic operational IT staff can access the data if assigned access to necessary operational tools. Chat transcripts are by default only tagged with a case id and searchable by agent, time and case ID through the application tools. If you have a Chat transcript ID retrieved, Vergic support staff can search logs to connect a visitor IP address to a chat session. This functionality is sometimes used to support customer in situations where threats have been involved. This is only possible for the duration of the log files lifespan.
3. User profile, by default the user profile only contains the visitor web session id and no personal data. The profile can be extended to contain personal data such as typically an e-mail address or social security number through account specific customization. If such customizations are done users with necessary privileges can access the data through the generic search methods for chat transcripts as described above.

4.2 Backups

Backups are done on a daily basis, backups of customer account data are stored for 30 days. Backups are encrypted. System back-ups are encrypted and not readable unless part of a system restore process.

5 ACCESS TO PERSONAL DATA – INFORMATION SECURITY

The Vergic datacenter, operated by GleSYS is secured by access control and reside in a premise designed for data center purposes. See Annex Data Center Security Management System for more information

GleSYS operational staff are not able to read any data in the servers, the data is encrypted and GleSYS personnel do not have access to data in unencrypted format.

Vergic operational staff are using a role-based system to define access levels, Vergic Data Protection Officer, i.e. Vergic CTO is responsible for delegation of these roles to individual employees.

By default, no access to personal data exists on the role.

Access to personal data stored in customer accounts requires that you are either a system super user, called an Account Administrator, and that the administrators has explicitly been granted access to a specific customer account data. Account Administrators are most often employees of the Data Controller given priviliges to configure and administer the solution.

Vergic operations server administrator team also has access when they are assigned as a member of the server operator administrator team.

Access to information within the Vergic Engage Platform is controlled through roles and authorizations. An authorization can be assigned to a role, allowing that role to perform an operation, such as reading some data or taking some action. In this sense, a role is a grouping of authorizations. Roles can be given to roles hierarchically and a user may have one or more roles.

For system level access, standard Windows domain controllers and Linux groups are used. Access to various logs are granted via membership to security groups, depending on the need for system access. Login is controlled through an internal SSO. Shell access to production systems is restricted to system administrators only and controlled via SSH public keys.

System logs are maintained in a central repository with restricted access on a need-to-know basis. The central repository logs are deleted automatically by a time-to-live that is set to 7 days or less.

6 RETENTION POLICY

Standard settings are defined below in 6.1. A retention policy, “time to live” can be set per account (customer) with regards to point 2 & 3. If other than standard this has to be defined in the individual DPA

6.1 Vergic Engage Standard & Vergic Engage Custom Settings

1. Logger data is stored for 7 days and thereafter deleted
2. Chat transcripts are stored for 14 days by default. Retention period is customizable and can be set to other lifespan as an account setting. Customer can decide the lifespan as a custom setting defined by the DPA
3. User profile, by default the user profile contains only the visitor web session id and no personal data. The profile can be extended to contain personal data such as E-mail address or Social security number by account specific customization
4. Back-ups are saved for 30 days

7 ERASURE OF DATA

Data will be automatically erased according to chapter 6. A request from an individual to erase personal data that request will be handled by the Data Controller (Vergic Customer) who will forward the individual request to Vergic. This will only be applicable in inside the retention period.

1. Logger data is stored for no more than 7 days and thereafter deleted. If requested logs related to an IP address can be deleted
2. Chat transcript are stored for no more than 14 days and thereafter deleted if not defined otherwise through a custom setting. Upon Request Chat transcripts can be individually deleted
3. User profile is stored alongside the chat transcript and will be deleted together with the chat transcript

Back up data are deleted according to the retention policy (see above). If an individual request for erasure would occur within 30 days from a system restore process has taken place that specific record will be deleted manually from the restored production database.

7.1 Erasure of data during an on-going chat session

See section 3.2.

8 SECURITY TESTING AND RISK MITIGATION

Application Information security is handled by roles, access rights and change/audit logs. Vergic has a set of governing documents that set policy for IT and application security management and Vergic CTO is responsible for conducting the tests and audits required in these documents to assure that the policies are maintained.