EU GENERAL DATA PROTECTION REGULATION (GDPR) WHITEPAPER

SafeNet Authentication Service & SafeNet Trusted Access

Version: 1.0

Date: 23 May 2018

Contents

Introduction

The purpose of this document is to provide guidance to Customers of Gemalto's SafeNet Authentication Service (SAS) and SafeNet Trusted Access (STA) around the data privacy and data protection requirements of GDPR. It also highlights the security controls and organizational measures that Gemalto has put in place to protect end users' personal identifiable information (PII) collected, processed and stored as part of providing these services.

Additionally, the SAS and STA security white papers provide further detail on some of the security measures we provide.

Gemalto, the Data Processor

Gemalto acts as a Data Processor while hosting and providing SAS/STA as cloud services ("Solution") to its partners and customers. Gemalto processes personal data of end users as required by the Solution and as agreed with its customers through our terms of service and data protection terms. End users' personal data is primarily used to associate an individual to an assigned token for processing authentication requests within SAS and to apply access related security policies within STA.

Gemalto's engagements as Data Processor has been elaborated in detail, which can be found here: https://www.gemalto.com/companyinfo/engagements-as-data-processor.

GDPR requires that Data Processors maintain records of data processing activities undertaken on behalf of a Data Controller, and mandates that they have security measures in place to ensure that data is adequately protected.

Gemalto's "Personal Data Protection Program" ensures that it strictly follows the appropriate standards and regulations. Gemalto has a comprehensive data protection framework and supporting security measures in place that assure GDPR compliancy.

Gemalto has amended its contractual terms for SAS and STA to reflect GDPR compliance. Customers of SAS and STA can access the amended agreements at the links below:

- Terms of Service – SAS and STA
- STA Data Processing Terms
- SAS Data Processing Terms

Customers, the Data Controller

The Data Controller is a business entity that determines the purpose and means of using their end users' personal data and also provides instructions to Data Processors for processing the personal data in order to provide a service and/or a solution to their end users.

Organizations that are using the service and who, as a result of this use, submit their end users' personal data to SAS/STA as part of providing multi-factor authentication and access management solutions for users accessing their business applications are considered Data Controllers.

This document describes some of the requirements for Data Controllers in relation to their use of the Solution, however it is not intended as an exhaustive list. It is up to the Data Controller to ensure that they are fully compliant with the GDPR rules and regulations with regard to use of Gemalto's solution and any other services pertaining to GDPR.

GDPR's accountability principle emphasizes an on-going responsibility for Data Controllers to demonstrate that they comply with the requirements of GDPR for privacy and security of their end user's personal data. The Data Controllers shall maintain complete, accurate and up to date written records of all activities carried out in relation to the "Right of Individuals".

Right of Individuals

The "Right of Individuals" define the legal rights of end users ("data subjects") to obtain:

- Confirmation that their data is being processed
- Access to their personal data or obtain a copy of the data
- Rectification or erasure of their data
- Restriction to the processing of their data

GDPR requires that the Data Controller shall provide information on action taken on "Right of Individuals" request to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months, where necessary, taking into account the complexity and number of the requests. The Data Controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Right to Consent

Under GDPR, it is required to provide intelligible and easily accessible consent forms to end users for collecting, processing and storing their personal data as part of the Solution. End users should be able to easily withdraw their consent, if required. Both Data Processors and Data Controllers should be able to demonstrate that consent has been given by the individuals to the processing of their personal data.

Gemalto and all customer and partner operators acknowledge and agree to Data Processing Terms (DPT), which identify the security rules for processing end user data as part of the Solution. The Terms of Service (TOS) is also provided as part of the Solution and available online for reference. Operators of the Solution provide consent during the first login to the SAS/STA Administrator Portal and every time an updated TOS or DPA is published.

The Data Controller should ensure its users have provided consent and that this consent can be withdrawn.

Right to Access

Under GDPR, it is required to provide evidence of what personal data is processed, where it is stored and how long it is stored within the Solution, including the backup data.

The Data Processing Terms of SAS/STA includes a Data Processing Addendum (DPA) that documents:

- the type of personal data collected
- the format in which it is stored
- the duration of its storage
- the security controls that are in place for its protection

The Solution requires only a minimal amount of personal data to identify the correct user with the correct token (OTP, GrIDsure etc) for authentication. The Solution allows the Data Controller to sync end user data from their user directory (Active Directory, LDAP etc.) or to manually enter the data into the Solution. Additionally a Data Controller can add optional personal data to the Solution.

The Solution provides an optional Risk Based Authentication component primarily used to determine if a more simplified authentication method can be used. When enabled, the Solution will collect further information on the end user such as IP address used to derive approximate geographic location, time of day, presence within the enterprise or not, etc. This data is collected and anonymized and used only for the purpose of authentication.

The Data Controller is responsible for sharing the data processing information as documented in the DPA to their end users, upon request.

Right to Rectification

Under GDPR, it is required to allow updates (i.e rectification, completion) of the end user's personal data within the Solution, upon request.

The Data Controller is responsible to fulfil this requirement upon receiving a request from their end users.

The Solution allows the Data Controller the ability to rectify any personal data within their control:

- Data synced by means of their data directory is updated automatically when the changes are made at the data source
- Data manually entered into the Solution must be changed by the Data Controller

In case of a disaster recovery scenario, where the Solution has been restored from a backup:

- Data synced by means of their data directory is updated automatically
- Data manually entered may need to be updated the second time by the Data Controller
    - The Data Controller is responsible to maintain a change log of their changes
    - The Data Processor is responsible to notify the Data Controller when a restoration has occurred and to what date in time

Right to Restriction of Processing

Under GDPR, it is required to stop processing the personal data of an individual for a period:

- if the accuracy of the personal data is contested
- if processing is unlawful and the data subject opposes the erasure, but requests the restriction of use
- the Data Controller no longer needs the personal data for processing, but they are required for establishment, exercise or defence of legal claims

The Solution allows the Data Controller the ability to control processing any personal data of individuals within the Solution:

- Data synced by means of their data directory can be locked in their data directory and is then updated automatically within the Solution
- Data manually entered into the Solution must be locked by the Data Controller

In case of a disaster recovery scenario, where the Solution has been restored from a backup:

- Data synced by means of their data directory is updated automatically
- Data manually entered may need to be updated a second time by the Data Controller
  - The Data Controller is responsible to maintain a change log of their changes
  - The Data Processor is responsible to notify the Data Controller when a restoration has occurred and to what date in time

Right to Be Forgotten

Data Erasure

Under GDPR, it is required to erase end user records from the Solution when the data is no longer required or if the end user explicitly requests to delete their data from the Solution.

The Solution allows the Data Controller the ability to erase/remove any personal data of individuals within the Solution:

- Data synced by means of their data directory is updated automatically within the Solution once removed from their data directory
- Data manually entered into the Solution must be removed by the Data Controller

In case of a disaster recovery scenario, where the Solution has been restored from a backup:

- Data synced by means of their data directory is updated automatically
- Data manually entered may need to be updated a second time by the Data Controller
  - Data Controller is responsible to maintain a change log of their changes
  - Data Processor is responsible to notify the Data Controller when a restoration has occurred and to what date in time

Removal of Virtual Servers

Each Customer account is associated to a virtual server within the Solution. Customers can also create virtual servers for their child accounts. When an account is closed, the operator or the administrator of the parent account should remove the virtual server. When a virtual server is removed, all associated data is also removed from the Solution.

The SAS Administrator Portal allows operators and administrators to delete virtual servers from the Solution. It is the responsibility of Partners and Customer to clean up and delete virtual servers that were created for trial/demo purposes and are no longer needed.

In the case of trial and demo accounts created by Gemalto for prospective customers, Gemalto will remove the account a reasonable period after the trial or demo is completed.

Data Security

Gemalto's "Personal Data Protection Program" strictly follows standards and regulations. It is based on security by design principle and provides guidelines for applying appropriate protection based on various data classification levels.

Data at Rest

Gemalto uses Transparent Data Encryption (TDE) technologies that encrypt the entire SAS/STA databases storing user data and authentication token data.

The log data generated by the Solution is stored in encrypted files/volumes. In addition, the log files that are collated in the log monitoring platform are also protected by storing them in encrypted files/volumes.

Data in Motion

The Solution uses secure communication protocols (like HTTPS, TLS) for inter-component connectivity. In addition to securing the communication, this also helps in preventing Man in the Middle (MitM) attacks.

Customers' data directories are synchronized with SAS using a lightweight synchronization agent. All communication between this synchronization agent and SAS is encrypted for enhanced security. In addition, a SSL secure tunnel is supported between the sync agent and the data directory server.

Data Backup and Recovery

Gemalto follows a formal Data Retention policy that ensures that the required data is retained according to the compliance requirements governing the Solution, which includes ISO 27001 and SOC2.

A daily back up of the data is conducted on a set of database servers to a separate local disk as well as hourly transaction log (TLOGs) backups. A full backup of the databases and associated transaction logs is also taken and encrypted from one of the data centres once a week. This backup is stored outside of the data centre for a period of 8 days and is used for disaster recovery purposes. A restoration test is performed annually. For this test, an encrypted backup is recalled from off-site storage and the data restored to a test environment.

In the event of Gemalto needing to recover from a backup, Gemalto will notify its Customers of the date and time the backup was taken. If the Data Controller's change logs show that a change was made to manually entered data, Customers should redo the modifications they executed during that period. In order to perform this activity, Customers shall maintain a registry (change log) that records all the changes they make in the Solution with regards to their end users personal data.

Conclusion

This document covers the key areas within the pages of GDPR that address data privacy and Right of Individuals as they pertain to the Solution. In general, both Data Controllers and Data Processors should review their organizational policies and practices in terms of personal data protection and ensure that GDPR requirements pertaining to other areas of their business are appropriately covered.

FAQ

1. Is the GDPR limited to businesses in the EU?

The GDPR applies not only to businesses which are actually located in an EU member state, but also to businesses located completely outside the EU if they process the personal data of EU residents and offers them goods and services, irrespective of whether payment is required or not.

2. What is the scope of the GDPR?

The GDPR lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data.

"**Personal Data**" means any information relating to an identified or identifiable natural; person 'data subject'; an identifiable 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, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

"**Processing**" means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. What is the difference between a Data Controller and a Data Processor?

- "**Data Controller**" means an entity who (either alone or jointly or in common with other entities) determines the purposes for which, and the manner in which, any Personal Data is, or has to be processed
- "**Data Processor**", in relation to Personal Data, means any entity (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller.

4. Does SAS/STA supports "Right of Data Portability"?

This is not applicable to SAS and STA. All the personal data comes from a data source maintained and managed by the Data Controller.