EU’S NEW GENERAL DATA PROTECTION REGULATION

INFORMATION FOR CSI CUSTOMERS

7.5.2018

CONTENT

1. EU'S NEW GENERAL DATA PROTECTION REGULATION

EU's new General Data Protection Regulation shall enter into force on 25th May 2018. The purpose of the new regulation is to increase the rights of individuals in relation to the management and processing of their personal data and to harmonize legislation across the EU member nations.

CSI is committed to follow the new regulation in its operations and to develop CSI Lawyer to support customers in their compliance with the regulation.

1.1. OBLIGATIONS OF CSI CUSTOMERS

CSI's customers act as data controllers for personal data registers maintained and managed in the CSI Lawyer software. In these cases, CSI never acts as a data controller but may act in the role of a data processor.

The data controller (the customer) determines the purpose and means of personal data processing. The data controller also ensures that the personal data is processed in accordance with the requirements of the regulation both technically and administratively.

The data controller must ensure that its operations are transparent to registered individuals. In practice, the controller is obliged to inform individuals of the processing of personal data, of the purpose and justification of the processing, the retention of data and the remedies. This information can be provided as a privacy policy.

In addition, the controller must ensure the accuracy of the personal data, limitation of the use of personal data and, in particular, the removal of unnecessary data. The controller is also responsible for facilitating the exercise of the rights of individuals. Individuals have for example the right to ask for their registered data, request correction of incorrect information and also require removal of information if there are no obstacles for it.

1.2. CSI'S OBLIGATIONS AS A SOFTWARE SUPPLIER

CSI helps customers to meet with their privacy obligations by developing the CSI software functionality as required.

Besides, per request of the customer CSI may act in the role of a data processor in the following situations:

- When processing conversion databases for the customer that is becoming a CSI user
- When processing test databases for the customer that is getting prepared to upgrade to a new CSI Lawyer version
- When establishing a remote connection or a database connection, for example, to troubleshoot the customer's problem situation or to implement the customer's request for changes to CSI Lawyer, or
- When merging or distributing CSI Lawyer databases in connection with the customer's mergers and acquisitions.

In the above cases the personal data to be processed by CSI may be

- personal data of the customer's clients, saved in the software, or any other personal data related to the customer's assignments, and/or
- personal data of the customer's employees i.e. CSI Lawyer users.

We have documented our way to operate as a personal data processor in the above situations, and clarified our practices in order to maximize the data protection.

2. CSI LAWYER'S SUPPORT TO GDPR COMPLIANCE

2.1. FUNCTIONALITY FACILITATING THE EXECUTION OF INDIVIDUAL'S RIGHTS

In CSI Lawyer each individual is established only once, which makes it easier to manage personal data and to comply with the GDPR requirements. For example, if an individual moves to another company, the new employer is updated into the individual's data to avoid duplicates.

CSI Lawyer facilitates executing the rights of individuals as follows:

INDIVIDUAL'S RIGHTS		CSI LAWYER'S FUNCTIONALITY
Access to personal data	Right to know if an individual's personal data is processed and to see it.	A personal data report lists the individual's personal data stored in the system. There are separate reports for customers and system users.
Rectification of data	Right to have outdated or inaccurate personal data corrected.	The basic system functionality covers editing of private persons' information.
Data portability	Right to ask for transfer of personal data to another data controller.	Personal data can be exported from CSI Lawyer in a format which can be imported to another system.
Objection to automated processing	Right to object to decisions based on automated profiling.	There's no automatic profiling. E.g. the conflict check collects the information but leaves the decision to a user.
Objection to processing	Right to object to the processing of personal data.	The marketing denial prevents adding an individual's information to mailing lists which are purely used for marketing purposes.
Right to be forgotten	Right to ask for the deletion of personal data unless prevented by e.g. valid agreements or applicable laws.	An individual can be removed from the system if there are no obstacles preventing it.

Personal Data Report and Data Transfer

From the version 7.0 on, CSI Lawyer offers a personal data report which lists an individual's data stored in the system: basic information, contact information and possible limitations such as a marketing denial or a service restriction. The personal data report is in a format which can be send to an individual as such. Besides the customer There is a report available of customers saved in CSI Lawyer as well as of system users.

The personal data can also be exported from the system in a format which can further be imported to another system.

Limitation of Data Processing

The CSI Lawyer 7.2 version will enable restrictions to sending of marketing e-mails to individuals who are added to mailing lists. If the "Marketing Denied" field has been checked in the private person's information, the person's contact information will not be added to the mailing lists that are used for marketing purposes.

Removing an Individual from the System

An individual's data can be removed from CSI Lawyer if there are no obstacles for the removal. Such obstacles might be e.g. assignments, time entries, activities, critical tasks, different kinds of invoices and payments.

In case an individual has information which prevents removing the data, that information must first be transferred to another customer (either to a private person or to a corporate customer). After the transfer, the system removes the individual from the database completely.

At the moment, it is not possible to remove users (employees) from CSI Lawyer's database. Instead, the information of a former CSI Lawyer user can be pseudonymised by replacing the user's id, name, e-mail or any other identifying information with a value which does not allow the individual to be directly identified without additional information which is properly stored separately from the CSI Lawyer software.

2.2. AUTHENTICATION OF CSI LAWYER USERS

CSI Lawyer users are authenticated either by using an Active Directory ID or a user id/password combination defined separately. This information is located in CSI Lawyer's database, where a power user can add or edit them. The password has been encrypted, so not even power users can see it.

Logging into the software also requires that the user's Active Directory ID has been defined adequate SOL Server permissions. Alternatively, it is possible to utilizea SQL login for which the SQL Server administrator has granted the corresponding permissions.

2.3. LIMITATION OF USER RIGHTS

CSI Lawyer's user management also enables limiting the visibility of the data. The CSI Lawyer power users have access to all information in the system; therefore we recommend keeping the amount of power users limited.

Navigation rights enable limiting the visibility of folders to different user groups. It is possible to define e.g. a user group for which private customers are not displayed at all. Such a group would only have access to corporate customer's contact persons.

An assignment of a private person can also be defined as an insider assignment, thus limiting its visibility to the assignment team members only.

2.4. KEEPING LOG ON PERSONAL DATA CHANGES AND REVIEWS

For monitoring personal data changes and reviews it is possible to activate a log functionality in CSI Lawyer. The change log is activated in the Settings (Database Management > Change History), where you can select a private person as a target to be monitored, and define the fields and e.g. specific subfolders to be monitored. If required, it is also possible to define additional restrictions to the monitoring.

Once the log functionality has been activated, it is possible to monitor the changes made to a private person's data in the history information. By default, CSI Lawyer displays when the private person's data has been created and when it has been changed. If required, it is also possible to see when the private person's data has only been reviewed without editing it. Changes made to the data in the private person's subfolders are displayed in the history of respective subfolders.

NOTE! Once the log functionality has been activated, it applies to **all** private persons saved in CSI Lawyer. Thus, when activating it, we recommend taking into account its possible impact on the system performance.

3. GDPR COMPLIANCE AT CSI HELSINKI

3.1. EXPERTISE AND RESOURCES

CSI's data security, any required changes and the implementation of new data privacy processes as part of the company's products and services are at the responsibility of CSI's management team.

The entire CSI staff has undergone the basic training about the requirements of the new regulation and is committed to comply with it in their work. Further training will be organized before the new regulation comes into effect, and in the future the employees will be provided with data security training at least once a year.

3.2. DATA PROCESSING AGREEMENTS

CSI understands it critical role as a processor of confidential personal data and takes the related responsibilties seriously. To complement our main contracts signed with customers, we'll provide our customers with a GDPR compliant data processing agreement.

We expect all the customers to sign the data processing agreement in order to ensure secure and GDPR compliant processing of personal data also after the regulation comes into effect on the May 25th 2018.

All our employees are bound by a confidentiality agreement, which applies to customer information, too.

3.3. USE OF SUBCONTRACTORS IN DATA PROCESSING

CSI strives for providing to customers services with the highest possible security and quality. In the provision of the services, we use subcontractors and partners which, according to the new general data protection regulation are also regarded as processors of personal data. However, the role of CSI's subcontractors as data processors is purely limited to the technical maintenance of the data repositories, and the subcontractors under no circumstances have the right to view or modify the personal data stored in the data repositories.

All CSI's subcontractors are aware and comply with the same or equivalent data security and privacy obligations to which we have been committed.

CSI's subcontractors are:

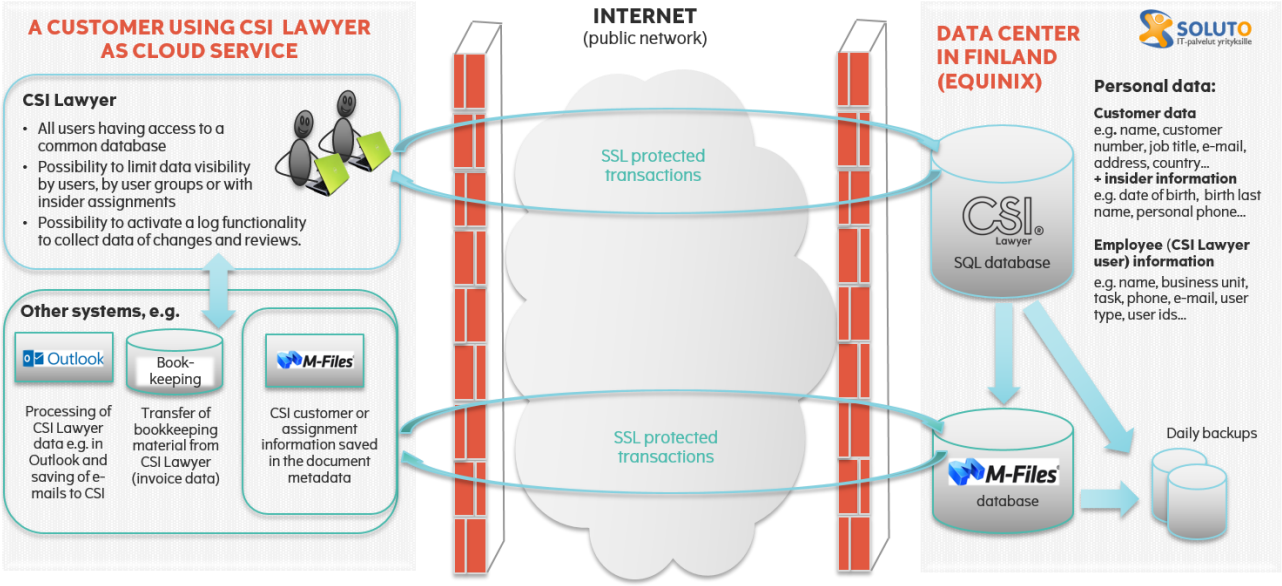
- Soluto Oy, 2084582-8 Cloud service provider
- SoftAvenue Oy, 1761128-9 Provider of IT services

3.4. SECURITY

The security and confidentiality of personal data is a key part of the new data protection regulation. We ensure the security of our customers' data by adhering to the best practices and standards in the industry, and constantly developing our readiness to create new security practices.

Security of the Cloud Service

In CSI's cloud service, the customers' data repositories are located in Helsinki, in a secure server environment which is ISO9001, ISO14001, ISO27001, ISO500001, OHSAS18001 and PCI-DCSS audited.



The server architecture is fault-tolerant, so the services remain available even if individual devices or services fail. A customer's database is backed up daily, and backups stored in a separate service. This ensures the recovery and integrity of data in case of a problem situation.

3.5. INTERNATIONAL TRANSFER OF PERSONAL DATA

CSI and CSI's subcontractors do not transfer personal data outside of the European Union.

4. CSI AS A DATA PROCESSOR

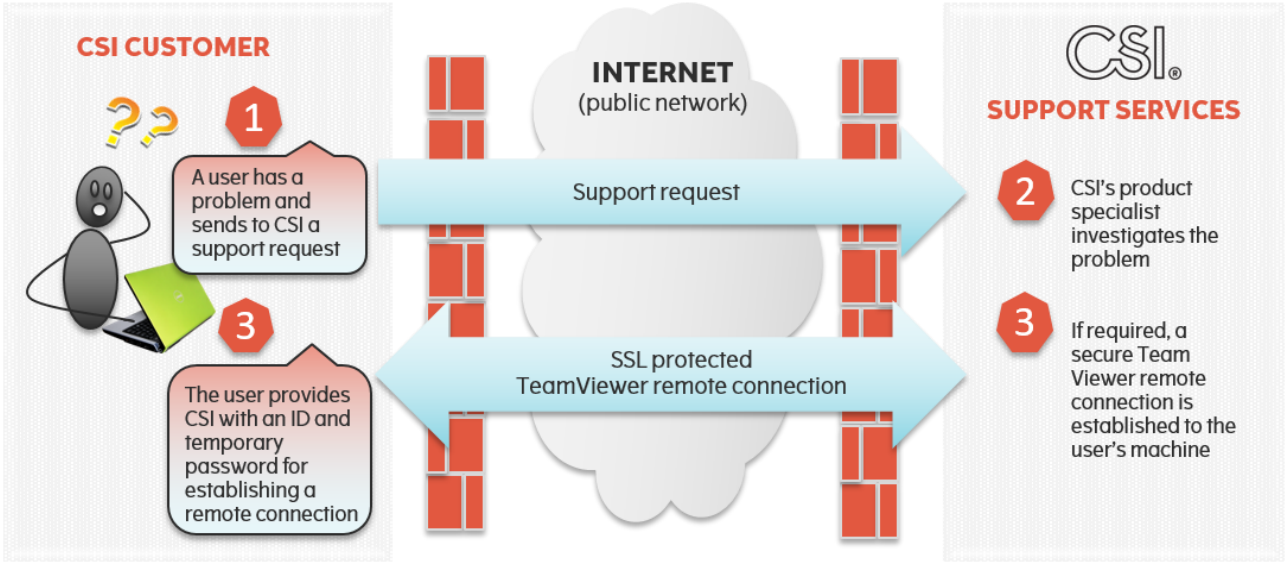
When processing the customer's databases or other personal data repositories CSI follows the following principles:

4.1. DATA PROCESSING

CSI processes the customer's databases and other information solely per request and on behalf of the customer. We process all the data safely and carefully, and pay particular attention to maintaining its accuracy. The customer's data is only processed by persons who have received adequate training in data protection and data processing.

4.2. SECURITY OF THE REMOTE CONNECTIONS

When establishing a remote connection to the customer's workstation or server, CSI primarily uses its own secure connection which the customer separately opens for the CSI specialist.



If the customer wishes to use any other connection, the customer ensures that the connection is secure and saves to a log all the required information.

When delivering new user IDs e.g. to a customer using CSI Lawyer as a cloud service, CSI always sends the related passwords in a separate e-mail.

4.3. DATA REPOSITORIES TRANSFERRED TO CSI

In case the customer's data repository has to be transferred to CSI for example for conversion or troubleshooting purposes, CSI will agree with the customer a secure transfer method.

All the customer's data repositories transferred to CSI are stored in a separate secure server environment with an access to nominated persons only.

4.4. STORING OF DATA REPOSITORIES

CSI does not store any customer data unnecessarily. Unless agreed otherwise, CSI destroys the customer's data repositories in its possession at the latest three months after the agreed or necessary actions have been taken and the data become unnecessary.

Per the customer's separate request, e.g. for the purpose of testing to be carried out on behalf of the customer, CSI can store the customer's data repository for a longer period. In such case the personal data in the customer's data repository can be pseudonymised to ensure the data security.

CSI takes no backups of the customer's data repositories which are in CSI's possession.

4.5. DELETING CLOUD CUSTOMERS' DATA REPOSITORIES

If the customer who has used CSI Lawyer as a cloud service, terminates the CSI agreement, CSI attempts to deliver a database stored in the cloud service to the customer and, after the delivery, destroys the customer's data repositories under its control. If the delivery is not possible, CSI retains

the customer's data repositories in its control for three months after the expiration of the agreement before deleting them.

4.6. NOTIFICATION OF DATA SECURITY BREACHES

If CSI detects any security incidents or other personal data security threats to the customer's personal data, CSI will inform the customer in writing without undue delay.

5. CSI AS A PERSONAL DATA CONTROLLER

CSI's principles as a data controller have been described as a privacy policy, available both as a separate document and in our website www.csihelsinki.com.

6. CSI'S GDPR SUPPORT TO CUSTOMERS

CSI supports the customers in any CSI Lawyer related questions regarding the new regulation and advices in the use of CSI Lawyer's data privacy functionalities.

This document will be complemented based on the questions received from the CSI customers. As the practices related to the GDPR compliance get more concrete, we'll develop CSI Lawyer's functionalities accordingly.

Customers are welcome to send questions related to the regulation as well as development wishes concerning CSI Lawyer's functionality to the CSI support team, support@csihelsinki.fi.