How SunFish Supports Customer Data Privacy

04 July 2018

Introduction

DataOn collects information in the course of our regular business operation through our websites and in provisioning of support to our customers and prospective customers. We also collect a variety of generic information on the usage of our systems through log files for performance monitoring and performance and/or usability improvements. This information is gathered when users access our system over the internet and is regulated in accordance with our privacy policy at https://www.dataon.com/privacy.

This document addresses the SunFish application for which a customer has purchased a license or subscribed to use. Data stored in SunFish is under the control of that customer and SunFish provides a variety of technologies and tools to assist customers in meeting their obligations for protection and control of that data. We advise that the customer is subject to a variety of legislation with regards to privacy including regulations of the country in which the customer is domiciled, countries in which they operate and, in some cases, countries of which their employees are residents.

On May 25th, 2018 the General Data Protection Regulation came into effect for the European Union member states and in the European Economic Area. Any organization that collects or processes personal data of an individual within the Union is subject to this regulation, regardless of the organization's location.

The information contained in this document is for general guidance only and is provided on the understanding that DataOn is not herein engaged in rendering legal advice. **The responsibility to adopt appropriate measures to achieve GDPR compliance rests with your organization as controllers in terms of the GDPR, and DataOn accepts no liability for any actions taken as response to this document.** As such, it should not be used as a substitute for legal or professional consultation.

GDPR regulation as well as specific country regulations address issues of data privacy and many countries are enhancing or are in the process of replacing these regulations. While most laws and regulations address similar issues and have similar compliance requirements, specific advice on regulations is outside the scope of this document. Some relevant national regulations are as follows:

-Indonesia Law No. 11 of 2008 regarding Electronic Information and Transactions, as amended by Law No. 19 of 2016 (the Electronic Information Law) and MOCI Regulation No. 20 of 2016 regarding Personal Data Protection in Electronic Systems
-Malaysia Personal Data Protection Act 2010 (PDPA)
-Philippines Data Privacy Act (DPA) RA 10173
-Singapore Personal Data Protection Act 2012 (PDPA)

DataOn is committed to ensuring privacy for data under our control as well as providing tools to our customers to help them ensure privacy and complying with applicable regulation. Securing data and ensuring privacy are essential concerns in provisioning HR applications and development regulations have not substantially changed the approach we take to security and privacy, however, new regulation has substantially increased compliance requirements for customers.

General Regulation Principles Specific to GDPR

In accordance with its general processing principles, the GDPR requires the processing of personal data to be lawful, proportionate, transparent, adequate, accurate, secure, confidential, limited in time and to designated purposes, and conducted in a responsible and accountable manner.

PERSONAL DATA

The GDPR explicitly defines what it means by the term personal data: any data that identifies or can be used to identify an individual. The term clearly includes metadata or other associated data such as IP addresses, cookies, or other identifiers that may trace back to an individual. The GDPR has broadened the known catalog of special categories of personal data to include genetic data, biometric data if used to uniquely identify a natural person, and data related to criminal convictions and offenses.

LAWFUL GROUNDS FOR PROCESSING

Processing personal data will be lawful only if one of the criteria for permission, as set forth in the GDPR, is met. If direct legal permission is absent, organizations need agreement from individuals whose data is to be processed. This agreement (or consent) must cover all purposes for which the organizations (intending to process the data) collect and process the data and must allow for the individual's right to withdraw consent at any time. This means that blanket consent or global consent is not valid for the processing of personal data.

Regardless of whether an organization is subject to the GDPR, these are generally good practices to follow. Data privacy and protection regulations are ever evolving, and it is in your organization's best interest to establish and maintain strict data privacy and protection policies. In the end, each organization must make its own interpretation of what it considers legal grounds for processing personal data. Chapter 2, Article 6, of the GDPR describes the lawfulness of data processing as follows and it shall be lawful only if and to the extent that at least one of the following applies:

• The data subject has given consent to the processing of his or her personal data for one or more specific purposes
• Processing is necessary for the performance of a contract in which the data subject is part of or in order to take steps at the request of the data subject prior to entering into a contract
• Processing is necessary for compliance with a legal obligation to which the controller is subject
• Processing is necessary in order to protect the vital interests of the data subject or of another natural person
• Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
• Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

ACCOUNTABILITY

The GDPR aims to improve accountability of those processing personal data and increase transparency of the data being processed. Despite its similarity in substance and structure to the current data protection legislation, the GDPR will take a much tougher line in helping enforcement. Penalties for noncompliance are remarkably high, including administrative fines of up to €20 million or 4% of an enterprise's global annual revenue, with potential damage claims and other legal liability risks designed to incentivize companies to enhance internal structures and processes to comply with the regulation.

DATA PROTECTION BY DESIGN AND BY DEFAULT

Under the terms of the GDPR, organizations must deliberately build in privacy, and both systems and processes have to adopt privacy by default. Organizations are obligated to ensure that the processing of personal data is for a specific purpose, and the organizations must demonstrate that data protection is at the heart of their IT framework and solution design.

TECHNICAL AND ORGANIZATIONAL SECURITY

Organizations are also obligated to implement all necessary technical and organizational measures to ensure a level of security appropriate to the risk of the processing for the data subjects. It is therefore necessary that the organization analyzes its internal IT asset landscape to identify and map data flows. This will help to ascertain the appropriateness of the security framework.

DATA SUBJECT RIGHTS

Organizations should be guided by the concept that the individual should know and always be able to identify what personal data is processed, by whom, for what purposes, and over what period of time. Thus, data controllers will need to actively provide certain general and specific information; this is in accordance with the GDPR's revised concepts of data portability and the individual's rights to access, refuse or object, or be forgotten. Organizations involved in processing personal data will therefore require robust internal processes with designated roles.

DATA GOVERNANCE

With an onus to clearly show customers, data subjects, and regulators that they are GDPR compliant, organizations must implement a host of systemic measures to reduce the risk of violation. Complexity grows when organizations need to keep track of every purpose for which personal data is being processed and when they need to ensure that all individuals have given their consent for each data processing use case. These measures must be built into existing IT infrastructures. Depending on the outcome of a data protection risk assessment, organizations should take measures to help maintain compliance. Such measures include the appointment of a dedicated data protection officer (DPO), the execution of privacy impact assessments (PIAs), and the adoption of regular audit procedures.

DATA RETENTION VERSUS DATA DELETION

Business systems, such as human capital management (HCM) systems, contain combinations of a multitude of records on both employees and other individuals, such as job applicants and contractors. A company's HCM system may, for example, store data related to job applications, payroll records, training history, compensation history, retirement plans, health information, and so on. Over time, a company's HCM system will accumulate a considerable number of records, many of which contain personal information related to individuals. The GDPR requires organizations to remove any personal data from their systems once this data is no longer needed for the course of business. You must do this, for example, when an employee leaves the company (including any transfer of employment to an affiliated company). In other cases, an employee may simply revoke their consent to a special data processing activity. At the same time, personal data obtained may still be lawfully processed on other legal grounds or be an integral part of records that are subject to retention times of 5, 10, or even 30 years. In such cases, the company needs to determine how to best store that data so it is not unnecessarily accessed but can still be retrieved by authorized parties.

DATA PROTECTION AS A PART OF LEGAL COMPLIANCE

Data protection requirements are only one subset of compliance requirements faced by a company. Data protection requirements need to be aligned with other applicable requirements, including tax legislation or industry-specific laws. Retention requirements are the best example. If more specific legislation defines that certain records, including personal information, need to be kept for 30 years, deletion of this data is not allowed. Organizations need to analyze their business processes with regard to all applicable legislation, and establish the appropriate technical and organizational measures to achieve and maintain compliance.

HOW SUNFISH SUPPORTS DATA PRIVACY AND COMPLIANCE

SunFish solutions are designed around comprehensive security and privacy standards. These already include many of the technical safeguards required to comply with privacy regulation and a range of business processes solutions which when used correctly can assist customers in meeting regulatory compliance requirements. We continue to enhance SunFish to provide our users with additional tools to simplify their compliance requirements.

COMPLIANCE SUPPORT

SunFish provides tools to simplify compliance for data that is in active use, while it is being retained after normal active use and how it is disposed when the data has reached its end of use.

Consent tracking

SunFish is in the process of releasing an additional tool to support tracking of employee agreements including consent forms. Consent trackings allows customers to create a consent form which can be presented to an employee each time they login to the application for their acceptance. Consent forms allow the employee to accept the form, defer their acceptance for some time, submit questions for clarification to a company appointed administrator or reject the form. Customers can select actions such as the maximum time an employee can defer their response before being blocked from accessing the application and whether to block employees from access if they reject the form.

Reporting on consent allows admin users to list who has accepted the form including time of acceptance and IP address used as well as who is still pending to accept.

Function Permissions

SunFish provides granular function access control to system functions with the ability to control a users ability to view, change and delete data. Access is generally configured to a specific function in the application, but can be granulary defined at the individual field level.

Data Permissions

SunFish allows permission of specific data in combination with data type to specific users and groups of users. Customers are able to report on access to data and revise data access to need to know rational changes over time. Reporting is provided for easy auditing of data and function permissioning. We advise establishing a process to regular review permissioning.

Change Logging and Reporting

SunFish logs updates to data performed by users and allows permissioned users to report on data changes including before and after states of the data. Permissioned users can view the type of data change, user that performed the change, time of the change, previous & new data, and other information. Filters can be applied by the user and specific reports are available to view data changes group by employee for example.

Personal Data Reporting

SunFish provides the ability to extract a comprehensive report on non transactional employee data for the purpose of complying with data requests from employees.

Personal Data Deletion

SunFish manages a large amount of employee data including the storing of transactional records and employee financial transactions that will require lengthy storage periods as a result of regulatory and audit requirements. The integrated nature of the data requires long term storage in order to maintain data integrity.

Once an employee ceases employment, they will enter a non active data storage phase. Employees no longer employed are segmented to a non active category for separate management. In order to provide the ability to comply with data deletion requests, SunFish allows for the deletion of employee personally identifiable information from records. Within the structure of the database tables, this data is directly substituted with a deletion identifier and is no longer viewable through the application.

Deleted data is stored in a separately encrypted format which is not application accessible. This data can later be recovered only by using the application secondary encryption keys. This data can additionally be purged from the application using the purge function described below.

Data purging

SunFish supports the ability to purge data from the database (in addition to archiving functionality). Purge functions can be scheduled or run manually. Purge functions permanently and unrecoverably remove data from the database. Data purging may be applied for the purposes of data cleansing to improve system efficiency or for the purpose of disposing of unused data to reduce liability and comply with data deletion requests. The recommended process is to maintain active data for the period required by regulation, then delete data using the Personal Data Deletion function and purge the encrypted data deletion records automatically based on a schedule of not less than one year.

Data portability and export

SunFish allows customers to extract data to unencrypted flat file formats to support the need for data portability. Functions are tailored to support data extraction for different purposes such as a system migration to another vendor, or requests by employees for data portability to, for example, subsequent employers.

TECHNICAL SAFEGUARDS IN SOFTWARE

Customers maintain complete and exclusive control over data stored in SunFish. While the usage of compliance support functionality described above assists customers in complying with privacy regulation, customers should also be informed and confident of the technical safeguards used to prevent unauthorized access to data.

Encryption of data at rest

SunFish software supports database level encryption which is applied as standard to all environments we operate and optionally for customer environments. In addition to database level encryption we additionally encrypt higher confidentiality data as it is submitted to the database to prevent accidental disclosure when highly permissioned users access the data for audit or other purposes. Passwords are only stored in hashed format and are not recoverable by decryption.

Encryption of data in transit

SunFish supports encryption of data in transit and we use standard SSL encryption for all environments we operate and encourage customers to implement encryption on environments they operate. SSL encrytption can be verified at https://www.ssllabs.com/ssltest/analyze.html?d=sf.dataon.com.

Segmentation of data storage and application

SunFish applications are configured with external access to the application for users and to block direct external access to file and database storage.

Use of Cookies

Cookies are small files which are stored on a user computer when the user accesses a web application. SunFish uses a variety of cookies in order to control access to the application and enhance the user experience. These cookies store user preferences and are used to identify the user to the application. The purpose of the cookies and summary of data stored in them is as follows:

Cookie	Use	Deleted on Logout
COID	Remember Company ID	No
CUSTOMIST	Remember Account Name	No
LANG	remember Language	No
SFUSRSESS_[URL]	SunFish User Session	Yes
SFUACCOUNT	remember Company|User|Language while logged in	Yes
SFCOLORSCHEME	remember Theme Preference	Yes
CSLFID	Confirm server session	Yes
JSESSIONID	Confirm server session	No
CFID	Confirm server session	Yes

Cookies do not contain personally identifiable information of users except for the SFUACCOUNT Cookie which contains the user's name and is deleted upon logout.

TECHNICAL SAFEGUARDS IN HOSTED SOLUTIONS

When SunFish subscriptions or perpetually licensed software is hosted by DataOn, we undertake industry best practices and additional methods to secure customer data. DataOn is certified for the ISO 9001 and 27001 standards which include certification of our hosting environments.

Period of notification

In the event that we become aware of a breach of our security resulting in unauthorized disclosure of customer data we conduct an impact analysis to determine what data was

breached and which customers are impacted. Upon completion of that analysis we inform customers. If we are not able to complete the analysis within 72 hours of becoming aware of the breach, we inform customers of the result of our analysis to that point.

Data copies and retention

We host client data on multiple servers simultaneously for redundancy or performance reasons. Access to customer files and database are provisions separately. Database access and encryption key are provisioned separately for each customer. In addition to production copies of data we maintain backups of data on separate equipment at the production site and at a physically separated backup site. These backups are maintained in accordance with our retention policy up to 6 months. Backups are stored in encrypted format. We also maintain copies of production data which are updated in accordance with our disaster recovery plan as frequently as each five minutes. The production copies of data used in our disaster recovery center comply with the same security standards as the production data center and updates to this data occur over a virtual private network in encrypted format.

Deletion requests

We do not respond to requests from employee of our customers to delete data. If we are obliged to respond we inform employees that they are required to contact the customer for data deletion. We store customer data on behalf of our customer and will delete all copies of customer data (in the entirety) upon a duly authorized order by the customer. In some cases deletion of some components of the data may require our manual intervention and multiple level of authentication resulting in a processing time of up to 30 days.

Separate customer databases

We store each customers' data in separate databases for which the database passwords and encryption key are electronically configured independently for that customer. In order to provision access we store reference information on each customer in a central database which does not contain confidential information of the company or information of employees.

Network Security

We operate multiple levels of firewalls on our networks and segment production networks from internal operations. We limit access to our internal networks to our technical staff required to perform maintenance functionality on our infrastructure and require they utilize a virtual private network and segmented security access point to gain maintenance access to production networks. We protect our network with intrusion protection devices and monitor access with an intrusion detection device.

Third party audits

We undertake third party audits of our compliance with ISO 9001 and 27001 standards and provide copies of our certifications to customers. We also perform internal scanning for security vulnerabilities and conduct internal penetration testing. We employ third party companies to conduct penetration tests of our hosting environment and software and provide audit report summaries to customers.