GDPR - Data Protection Impact Assessment

This document follows the template provided by the European Union at https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf

Definitions

In this document:

- “DPIA” stands for “Data Protection Impact Assessment”.
- “CRM” stands for “Customer Relationship Management”
- “Customer” are companies that are using Sharework (they have a “Sharework Workspace”)
- “Co Workers” are users in the Customer that have a Sharework account (they are Sharework Users)
- “Approved Partners” are Partners of the Customer that are also using Sharework and have been approved

Policy

This document must be revisited at least annually to make sure it is aligned with the current scope of Sharework’s activities.

Need for DPIA

As a data processor using New Technologies, Sharework needs to perform a DPIA.

There a 3 different type of personal data processed by Sharework:

- “User data”, provided by the user himself
- “Sales employee data”, provided by the customer (employer of the sales)
- “Contact data”, provided by the customer in a connected CRM data source

Description of the processing

Nature of the processing

All personal data is encrypted at rest, regardless of the database type it is stored in.

User Data

User Data is collected and maintained by the user.

It is stored in Sharework’s relational database, as well as in Sharework analytics database and search index.

It is exposed to Co Workers and Approved Partners

Sales Employee Data

Sales Employee Data is collected from a data source uploaded (CSV) or connected (CRM) by a Customer organisation. For CRM data sources, an API exposed by the CRM system is used to collect and maintain the data.

It is stored in Sharework’s relational database.

It is exposed to Co Workers, and to Approved Partners

Contact Data

Contact data is collected and maintained through a connected data source (CRM) API.

It is not directly exposed to anyone, except for job titles, that are exposed to Co Workers and Approved Partners for which the sharing has been approved.

All data is stored after obfuscation (except Job Titles) in a data lake, then in a relational database.

Scope of the processing

User Data

- First Name

- Last Name
- Professional Email
- Professional Phone
- Work Experience
- Job Title

Sales Employee Data

- First Name
- Last Name
- Professional Email
- Professional Phone

Contact Data

- Email
- Phone
- Job Title

Context of the processing

User Data

User data is collected directly from the Users, first when they register, then when the complete and update their profile in the dedicated functions. They are informed about Sharework Data Policy at sharework.co before registration, then informed again and required to approve right after they register.

Sales Employee Data

Sales Employee data is collected using APIs, on behalf of the Customer that is their employer. It is the Customer's responsibility to ensure that Sales People are informed about the use of their personal data in the CRM and connected applications.

Contact Data

Contact data is collected after the Customer (acting as Data Controller) has been informed and accepted Sharework data protection policy, including nature of collected data and the purpose.

Purpose of the processing

User Data

Authenticate and identify users in the system.

Sales Employee Data

Share account owner information to Approved Partners.

Allow direction communication between Customer Sales Employees and Approved Partners Sales Employees.

Contact Data

Identify matched accounts in Approved Partners' data sources.

Identify matched accounts in Approved Partners' data sources that share contacts.

Identify typical personal targeted by Approved Partners' sales employees.

Consultations

Sharework Lawyers have been consulted in the process of defining the use of the personal data as described in the previous section.

Compliance and Proportionality measures

User Data

First Name and Last Name are required to clearly identify the user.

Email is required to authenticate the user.

Work Experience, Job Title are required to identify the role of the user and make sure the proper configuration is set to serve the right use case (including privileges).

Sales Employee Data

First Name and Last Name are required to clearly identify the user.

Email and Phone Number are required to communicate with the Sales Employee.

Contact Data

Email and Phone Number are required to identify matching records within multiple Approved Partners' CRM.

Job Title is required to identify typical persona of Approved Partners

Risks

Assessment

Source of risk and nature of potential impact on individuals	Likelihood of Harm	Severity of Harm	Overall Risk
Leak of User email and/or phone number can lead to spam or fraudulent emails	Remote	Significant	Low to medium
Leak of Sales Employee email and/or phone number can lead to spam or fraudulent emails	Remote	Significant	Low to medium
Leak of Contact email and/or phone number can lead to spam or fraudulent emails	Remote	Significant	Low to medium

Measures

Risk	Measure	Effect on Risk	Residual Risk
Leak of User email and/or phone number can lead to spam or fraudulent emails	Standard security	Reduced	Low
Leak of Sales Employee email and/or phone number can lead to spam or fraudulent emails	Standard security	Reduced	Low
Leak of Contact email and/or phone number can lead to spam or fraudulent emails	Non-reversible Hashing /Encryption	Eliminated	None