biobord operating model

Management documents 3: Data Balance Sheet

Published on 15.1.2020

Table of Contents

[1. Introduction 2](#_Toc29887295)

[2. Overview of Personal Data Processing 2](#_Toc29887296)

[2.1 Data Inventory 2](#_Toc29887297)

[2.2 Personal Data Flow Mapping 2](#_Toc29887298)

[2.3 Organization of Data Protection 3](#_Toc29887299)

[2.3.1 Data Controller 3](#_Toc29887300)

[2.3.2 Data Protection Officer 4](#_Toc29887301)

[2.3.3 Monitoring and Advisory Group 5](#_Toc29887302)

[3. Rights of Data Subjects 6](#_Toc29887303)

[3.1 Right to Transparent Information 6](#_Toc29887304)

[3.2 Right of Access 6](#_Toc29887305)

[3.3 Right to Rectification and Erasure 6](#_Toc29887306)

[3.4 Right to Data Portability 6](#_Toc29887307)

[3.5 Right to Restriction of Processing 7](#_Toc29887308)

[3.6 Right to Object to Processing, Automated Decision-Making and Profiling 7](#_Toc29887309)

[4. Regular Destinations of Disclosed Data 8](#_Toc29887310)

[5. Anonymization and Pseudonymization of Personal Data 8](#_Toc29887311)

[6. Risk and Impact Assessment 9](#_Toc29887312)

[7. Availability of Documents 9](#_Toc29887313)

# 1. Introduction

The purpose of Biobord Data Balance Sheet is to demonstrate to the supervisory authority and to our network partners how we have organized the processing of personal data collected in Biobord platform. This ‘Data Balance Sheet’ considers both the national legislation in Finland and the EU General Data Protection Regulation.

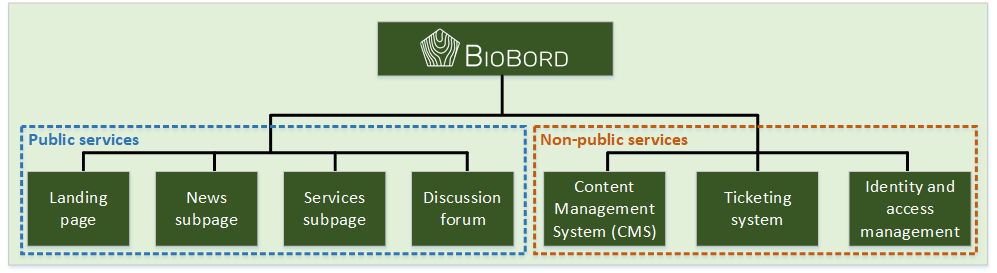
# 2. Overview of Personal Data Processing

## 2.1 Data Inventory

With regards to the Biobord platform, JAMK University of Applied Sciences is the owner of the Biobord user register with information regarding the name, email address, affiliation to coworking groups in the Biobord Forum and rights to Content Management System of Biobord.

## 2.2 Personal Data Flow Mapping

Biobord is a web platform hosted in Amazon Web Services (AWS) in Stockholm, Sweden. Platform has the following publicly viewable pages as presented in figure 1: Landing page, services subpage, news subpage, discussion forum. First three services can be viewed without user registration and authentication. Discussion forum has both public and non-public categories and only public categories can be viewed without user authentication. All non-public services require registered user to enter credentials (username and password) in order to use them.

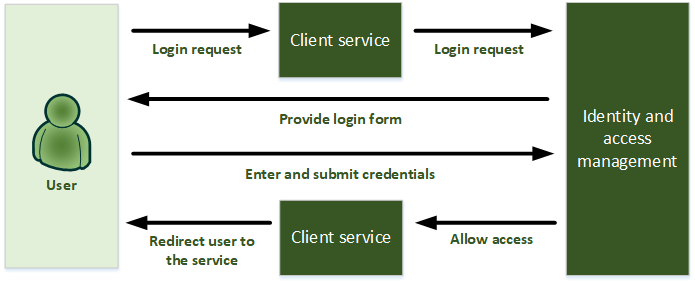


**Figure 1. Biobord web platform structure**

Registered user information is handled in identity and access management service. User is required to login to any of the services once and after successful login user session is established. Active user session enables user to view any service which requires authentication in Biobord. User can change user account settings any time by logging in to identity and access management service. Non-public services have two access conditions that must be met in order for user to use the service:

* User must have a registered user account
* User must belong to a user group which has access rights to the service

All non-public services act as a client service for the identity and access management service. Each time user wants to login to the platform, login form is presented by the identity and access management system. As a part of a login process, identity and access management system checks user credentials and informs the client service for successful or unsuccessful login event.



**Figure 2. User data flow in authentication process**

## 2.3 Organization of Data Protection

### 2.3.1 Data Controller

At JAMK University of Applied Sciences, we have allocated the responsibility for data protection management in relation to the national Finnish and EU legislation, the wide scope of the work on data protection and the fact that it involves every person in our organization. The aim of our data protection organization is to take work on data protection as part of the operative activities of our organization and to report on matters such as new projects relating to personal data processing.

The responsibilities, obligations and rights relating to personal data are defined according to roles. The data controller and the data processor are distinguished from one another and determined according to the circumstances. The data subject is the person whose personal data is under discussion, in this case the registered Biobord user.

For all personal data files, a description of file or privacy policy must be produced. This document contains information on the controller but also on the person in charge of matters related to the data file or the controller’s representative who oversees the services related to the rights of data subjects. The fact that the controller appoints a data protection officer does not affect the controller’s responsibility for the data file.

The Data Protection conducts in Biobord platform have been assigned in line with the overall data protection principles of JAMK University of Applied Sciences. However, this document is limited to viewing the data protection protocol and system with regards to Biobord platform administrated by JAMK University of Applied Sciences.

### 2.3.2 Data Protection Officer

With regards to Biobord Platform, the data protection officer at JAMK University of Applied Sciences assigned to the task for the duration of the RDI2CluB project are Anna Aalto as the project manager of RDI2CluB project and Antti Häkkinen as the expert in charge of the technical development of the platform.

The data protection officers have independent position in the organization. They report directly to the RDI2CluB Steering Committee as the Data Security Group of Biobord and the respective directors of the JAMK Institute of Bioeconomy and JAMK Institute of Information Technology. The data protection officers are involved on daily basis in the operative management and user guidance on Biobord platform.

The data protection officers have received expert consultation on data protection law and practice with regards to application for Biobord Platform. They are also supported by the data protection organization of JAMK University of Applied Sciences in specific questions concerning application of data protection processes. During the RDI2CluB project lifetime, the data protection officers have dedicated work time for the daily management of the Biobord platform, including data protection related tasks.

The data protection officers are administrators of the Biobord Platform having access to the personal data and processing operations. The data protection officer is obligated to maintain secrecy. He or she may not be dismissed or penalized for performing the tasks of the data protection officer, and he or she may fulfil other tasks and duties in addition to those of the data protection officer, as long as any such tasks and duties do not result in a conflict of interests.

The data protection officer has the following tasks:

* The implementation and application of the General Data Protection Regulation in the organization
* Participation in the management of data protection risks
* Provision of information and advice to the organization in all matters related to data protection
* Supervision of the production, availability and maintenance of documentation
* Monitoring the implementation of the notification obligation
* Support of and monitoring of the performance of the data protection impact assessment
* Cooperation with the supervisory authority
* Construction of a data protection awareness program and personnel training
* Support of the realization of the rights of data subjects
* The appropriate observation of risks involved in processing operations
* Planning and implementing operation control
* Reporting to organization management on the state of data protection and the related needs for development
* Participation in other tasks supporting data protection appointed by organization management

In order to maximize support to the controller, the data protection officer should be able to perform the abovementioned tasks and the related planning, monitoring and reporting duties as independently as possible. Being aware of the current state of the organization’s data protection is a crucial part of the controller’s accountability. The data protection officer produces an annual report that includes all matters related to data protection and personal data processing.

This Data Balance Sheet gives an overall picture of the current state of the personal data processing and data protection at the organization. It helps the management to monitor and assess the organization’s current state and allocate resources to its development.

### 2.3.3 Monitoring and Advisory Group

RDI2CluB Project Steering Committee represented by 12 partners is acting as a monitoring and advisory group of the Data Protection Organization of Biobord platform during the project lifetime until end of September 2020. The Project Steering Committee Rules of Procedure have been stipulated in the ‘Quality assurance and monitoring plan’ of the RDI2CluB. The RDI2CluB Project Steering Committee meets twice a year with meetings schedules for December 10, 2019, and May 2020 as online meetings carried out via Zoom web meeting platform. JAMK University of Applied Sciences is chairing the meetings while the secretary duty is alternating between other partners.

The following issues concerning data protection are brought to the agenda of the monitoring and advisory group:

* Review of the Customer register privacy statement
* Review of the Data Balance Sheet (incl. risk register)
* Review of notification of anomalies (and responses)
* Review of the annual work plan for data protection monitoring

# 3. Rights of Data Subjects

## 3.1 Right to Transparent Information

The controller must provide any information relating to personal data processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information must be provided in writing, or by other means, including, when appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is verified by other means. The controller must facilitate the exercise of data subject rights.

## 3.2 Right of Access

Everyone has the right to inspect the data on them or a child in their custody in a personal data register. Data subjects have the right to inspect what data on them have been stored in the data file or a right to a notice that the file contains no such data. In addition, after a sufficiently detailed and accurate request has been submitted, data subjects have the right to access the data concerning them stored in the personal data register. The controller must at the same time provide the data subject with information of the regular sources of data in the register, on the uses for the data in the register and the regular destinations of disclosed data.

The right of access must be exercised in person, and it cannot be performed through an attorney or other agent. The data may be stored in different locations and formats. This does not, however, prevent access to the data. Furthermore, exercising the right of access does not require the ability to name a specific data file. Data subjects may exercise their right of access once a year without charge. The request for access must be delivered in written form and with the subject’s signature to the address specified in the data protection statement of the controller.

## 3.3 Right to Rectification and Erasure

Data subjects have the right to obtain from the controller without undue delay rectification to inaccurate personal data concerning them.

Data subjects also have the right to obtain from the controller the erasure of personal data concerning them without undue delay. However, this right does not apply to statutory registers or data that are stored under legal obligations.

## 3.4 Right to Data Portability

According to the EU General Data Protection Regulation, data subjects have the right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller. Data subjects have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

The right to data portability applies to data that subjects have consciously provided for the controller, such as data in an electronic order form, and to the raw data related to the use of an electronic service, such as location data, search and purchase history and contact persons. The right to data portability is narrower in scope than the right of access, and it does not apply to data derived or concluded from raw data.

## 3.5 Right to Restriction of Processing

Data subjects have the right to demand restriction of data processing. According to Section 3, Article 18 of the General Data Protection Regulation, data subjects have the right to obtain from the controller restriction of processing where one of the following applies:

* (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
* (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
* (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims;
* (d) the data subject has objected to the processing of personal data pending verification whether the legitimate grounds of the controller override those of the data subject.

When processing has been restricted for the reasons mentioned above, such personal data must, with the exception of storage, only be processed with the data subject’s consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

## 3.6 Right to Object to Processing, Automated Decision-Making and Profiling

Data subjects have the right to object to personal data processing, automated decision-making and profiling.

# 4. Regular Destinations of Disclosed Data

In individual cases, necessary user data may be disclosed for legal purposes to authorities. JAMK University of Applied Sciences discloses data on a customer or stakeholder to the designated party if the data subject so requests or if a competent authority requires JAMK University of Applied Sciences on legal grounds to disclose specified data in the database in our possession. Data may also be transferred to the marketing register of JAMK University of Applied Sciences with the specific approval of the data subject.

There are currently no regular destinations of disclosed data outside the data controller. Within the RDI2CluB partnership, user data overviews can be used to analyze the community building progress of Biobord platform. However, this usage does not involve sharing or transferring any contact information or names of the users.

# 5. Anonymization and Pseudonymization of Personal Data

Personal data must be kept in a format which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. In practice, this means that organizations must anonymize personal data if they are to be kept beyond the purpose for which they were originally collected. JAMK University of Applied Sciences does not engage in activities for which personal data would be archived for other than their original purposes, creating no need for anonymization or pseudonymization.

# 6. Risk and Impact Assessment

The identified risks related to the user register concern use of user data for marketing purposes against user’s prior approval. All in all, the risk and related impact are perceived low. Risk register presents the results of the risks and impact assessment on the Biobord user register.

**Table 1: Risk Register**

|  |  |  |  |
| --- | --- | --- | --- |
| Identified risk | Impact of the risk | Likelihood of the risk | Control measures |
| Accidental human interference - deletion of critical files | High | Low | Data Backups |
| Malicious human interference - database breach | High | Low | Up-to-date identity and access management software as well as hardened server platform |
| Data loss due to system failure or natural disaster | High | Low | Distributed data servers and data backups |
| Leak of user credentials | Medium | Low | Two factor authentications enabled for login |

# 7. Availability of Documents

The Customer Register Privacy Statement for our personal data registers is publicly available at Biobord platform. This Data Balance Sheet is available on request from the Data Protection Officer