# ARES - Privacy Impact Assessment (PIA)

# Document Information

| | |
|---|---|
| **Titel** | **ARES - Privacy Impact Assessment (PIA)** |
| **Version** | **1** |
| **Validity Date** | **28-4-2018** |
| **Periodic Review** | |
| **Author** | **L. de Hooge** |
| **Reviewer 1** | **C. Kleiberg** |
| **Review Date 1** | **30-4-2018** |
| **Reviewer 2** | **Pharox Automatisering B.V.** |
| **Review Date 2** | **19-4-2018** |
| **Reviewer 3** | |
| **Review Date 3** | |
| **Approved by** | **C. Kleiberg** |
| **Release Date** | **1-5-2018** |
| **Classification** | **confidential** |

# Abbreviations and Glossary

### Glossary

| Term | Meaning |
|---|---|
| Data Controller | Any person or body which collects processes or uses personal data on his, her or its own behalf, or which commissions others to do the same. She is liable to the data subject and is in a legal relationship towards the data subject which permits the processing of the data. |
| Data Processing | Means the combination of all data processes to realize the purposes of collection, processing or use of personal data. |
| Data Protection Office | The Legal Expert on Data Protection and the Data Protection Officer |
| | |
| SharePoint | Platform to exchange documents |

**Table 1 Glossary**

# Contents

# 1 Document Overview

## 1.1 Definitions

**Personal Data** designates 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 identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

**Sensitive Personal Data** designates data that refers directly or indirectly to the racial or ethnic origin, political opinions, philosophical or religious opinions, trade union memberships, health or sexual life and orientations, biometric information, financial information such as bank account or credit card or debit card or other payment instrument details.

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

**Transfer of Personal Data** designates the disclosure of Personal Data to any third party, the transmission of such data to any third party, or the process of making such data available to any third party in any form for inspection or retrieval. For the sake of clarity, potential remote access to Personal Data hosted in another jurisdiction constitutes a Transfer of Personal Data.

## 1.2 Personal data protection and privacy key principles:

This is the checklist of some key principles that have to be kept in mind and shared within the Customer, the operational bid/project teams and the data protection office:

- Is the data processing / project **legitimate** and **fair**?
- Is the data processing / project **relevant** and not **excessive**?
- Are the data **proportionate with the purpose**?
- Is the **data retention period reasonable**?
- Where Sensitive Data are processed, necessary additional **security** measures are provided?
- Personal Data Transfers are appropriately **framed**? (where applicable)
- The security measures in place are **appropriate (trust and verify)**?
- The **data subjects' rights** are taken into account (information, access, deletion, correction, opposition, right to be forgotten?
- Are there any explicit **requirements regarding protection of personal data** from the customer?
- Are there any explicit requirements **regarding data security** from the customer?

# 2 Document Overview

## 2.1 Change History

This document is maintained by the Author.

| Date | Author | Version | Change description |
|---|---|---|---|
| 07-06-2017 | L. de Hooge | 1 | Initial document |

**Table 1 Change history**

## 2.2 Reviews and Review- Cycle

This document is to be verified once a year for keeping it up-to-date in terms of relevance and validity and modified as necessary. Responsibility for this purpose is taken by the author of this document.

The next scheduled review of this document is to take place on:

Review-History:

| Version | Review Datum | Review Team |
|---|---|---|
| 1 | 30-4-2018 | C. Kleiberg |

**Table 2 Review Historie**

Additional reviews are also documented in this chapter.

## 2.3 Objective

This Description of Data Processing describes

- the purposes of collection, processing or use,
- the legal grounds,
- the recorded personal data,
- the extent and the recipients to which the data are transferred,
- issued subcontractors,
- data retention periods,
- a list of persons or group of persons entitled to access,
- a description of technical and organizational measures to assure an appropriate level of security of data and
- an assessment of the data processing by the Data Protection Office.

## 2.4 Scope

This document is valid for ARES.

## 2.5 Monitoring and Enforcement

The author of this document is responsible to provide the accurate information of the documented processing. The Data Protection Office in cooperation with the author and where appropriate with other consulting persons will perform the data protection assessment.

If case of changes in the processing the author is responsible to review the document and to get a new data protection assessment.

## 2.6 Distribution List

As a confidential document the distribution list is restricted to:

- Management
- Staff divisions
- Members of the Security Management Circle
- Data protection coordinators
- Workers council

# 3 2. Privacy Impact Assessment for customer

## 3.1 Section 1 – Basic information about the processing

| Question | Answer |
|---|---|
| a. Name of the requester (Bid manager or equivalent / Sales manager / key contact) | C. Kleiberg |
| b. Service Line / Department | N.A. |
| c. Name of the project, contract or Bid | ARES |
| d. Customer name (full name and address if available) | SAB Stichting Afvalstoffen & Vaardocumenten Binnenvaart |
| e. Purpose of the processing (what does the processing do?) | Algemeen registratie system/database |
| f. Does the processing involve sensitive personal data? | ☐ No ☒ Yes |
| g. Does your request relate to a new project or are you regularizing a situation? | ☐ New project (not launched yet),<br>☒ Regularization (already launched),<br>Please specify date of initial launch:<br>01-09-2009 |
| h. Do you use a subcontractor? | ☐ No ☒ Yes<br>If yes:<br>☒ Pharox Automatisering B.V. |

**Table 3 Basic information about the processing**

## 3.2 Section 2 – Privacy Impact Assessment for Customer, Details and DPO and DPLE comments / corrective measures

| | Answer (to be completed by requester) | Comments and suggested corrective measures (to be completed by Global / Local DPO and or DPLE) |
|---|---|---|
| **A. General information about the processing / project** | | |
| **A1. PIA # - To be completed by DPO Format: PIA + P (for Processor) + Country Code (e.g. ES for Spain) + Number of receipt) – for example: PIA-P-ES-013** | | |
| **A2. Intended / Expected Date of Customer implementation** | **01/09/2009** | |
| **A3. Name of software / application and type of platform (e.g. Mobile App, SaaS, License, ...))** | **ARES** | |
| **B. Data processed and purpose of the processing** | | |
| **B1. Purpose of the processing / project (what does the processing do?)** | **Registration of data related to the administration of inland shipping** | |

| | | |
|---|---|---|
| **B2. Categories of persons whose data will be processed on behalf of the Pharox customer** | ☐ **Employees of the Pharox customer**<br>☒ **Customers of the Pharox customer**<br>☐ **Providers**<br>☐ **End-Users**<br>☐ **Members**<br>☐ **Visitors**<br>☐ **Other** – Please specify: | |
| **B3. "Standard" Categories of data processed**<br>**(please include a complete list of categories of data processed in annex if possible)** | ☒ **Identification data**<br>☐ **Personal life**<br>☒ **Professional life**<br>☒ **Connection Data**<br>☐ **Location data**<br>☐ **Account profile** [1]<br>☐ **Other** – Please specify: | |
| **B4. "Sensitive" categories of data processed**<br>**(please include a complete list of categories of data processed in annex if possible)** | ☒ **Social Security Number or National**<br>☐ **Biometric and/or Genetic data**<br>☒ **Banking and financial data**<br>☐ **Racial or ethnic origin**<br>☐ **Philosophical, political or religious opinions**<br>☐ **Trade-union affiliation** | |

[1] Local need in some countries

| | | |
|---|---|---|
| | ☐ **Health information**<br>☐ **Sexual life**<br>☐ **Criminal Offenses & sanctions**<br>☐ **Data telephone intercepts** (authority of justice)[2]<br>☐ **Other** – Please specify: | |
| **B5. Origin of the data** | ☒ **From the Pharox customer**<br>☒ **From the data subject directly**<br>☐ **From an existing processing :**<br>☐ **From data broker:**<br>☐ **From other origin –** specify: | |
| **B6. Has a term of retention been defined by the customer for all categories of data?** | ☒ **No** ☐ **Yes** | |
| **B7. Defined term of retention of data** | **Deletion/Destruction of the data, specify the term:**<br>☐ **Term of the agreement –** specify:<br>☐ **Archiving –** specify conditions and term**:**<br>☐ **Pseudonymisation** – specify conditions: | |

[2] Local need in some countries

| | | |
|---|---|---|
| | ☐ **Anonymization -** specify conditions and term:<br><br>☒ **Other –** specify:<br>Deletion / destruction of data upon formal request from SAB | |
| **B8. How is the data defined retention period enforced by Pharox?** | ☒ **Manual deletion**<br>☐ **Automatic deletion**<br>☐ **Other –** specify: | |
| **C. Subcontracting & International Transfers, Access to the data** | | |
| **C1. Is the processing / project / service (or parts of it) provided by external providers?** | ☐ **No** ☒ **Yes** – Names: | **Databarn Rivium B.V.**<br>**Successfully NL B.V.** |
| **C2. If yes, specify for each provider (a, b, c,…) the name of the legal entities, the address, the services provided, and the contact persons (if any)** | **Services such as development, testing, hosting, support, maintenance, remote access, on site services, other…**<br><br>**Supplier A:** Databarn Rivium B.V.<br>Data center / hosting services<br>Databarn Rivium B.V.<br>Rivium Boulevard 62<br>2909LK Capelle aan den IJssel<br>**Supplier B:** Successfully NL B.V.<br>System management services | |

| | | |
|---|---|---|
| | Successfully NL B.V.<br>Diakenhuisweg 27<br>2033 AP Haarlem<br>**Supplier C:**<br>N/A | |
| **C3. Where are the providers' processing activities (i.e. servers, databases and/or persons who have access the personal data, etc.) located?** | **Supplier A:**<br>☒ **EU –** Specify by country which data or data categories: **NL, data categories specified by SAB**<br>☐ **Non-EU** – Specify by country which data or data categories**:**<br><br>**Supplier B:**<br>☒ **EU –** Specify by country which data or data categories: **NL, data categories specified by SAB**<br>☐ **Non-EU** – Specify by country which data or data categories**:**<br><br>**Supplier C:**<br>☐ **EU –** Specify by country which data or data categories:<br>☐ **Non-EU** – Specify by country which data or data categories**:** | |

| | | |
|---|---|---|
| **C4. If the provider (or any of its services) are located outside the EU, please specify which safeguards are implemented** | **Supplier A, if located outside EU:**<br>☐ **EU recognized adequate country**, specify :<br>☐ **EU Standard Contractual Clauses**<br>☐ **Specific data transfer agreement**<br>☐ **Third party Binding Corporate Rules**<br>☐ **EU-U.S. Privacy Shield**<br>☐ **Other**, specify :<br><br>**Supplier B, if located outside EU:**<br>☐ **EU recognized adequate country**, specify :<br>☐ **EU Standard Contractual Clauses**<br>☐ **Specific data transfer agreement**<br>☐ **Third party Binding Corporate Rules**<br>☐ **EU-U.S. Privacy Shield**<br>☐ **Other**, specify :<br><br>**Supplier C, if located outside EU:**<br>☐ **EU recognized adequate country**, specify : | **N/A** |

| | | |
|---|---|---|
| | ☐ **EU Standard Contractual Clauses**<br>☐ **Specific data transfer agreement**<br>☐ **Third party Binding Corporate Rules**<br>☐ **EU-U.S. Privacy Shield**<br>☐ **Other**, specify : | |
| **D. Implementation of data subject rights** | | |
| **D1. Do we provide a service to the client where we assist in providing data subjects with information about the purpose of this processing?** | ☒ **Yes** ☐ **No** | |
| **D2. If yes, how will information about the purpose of this processing be provided to data subjects?** | Webbased portal mijn-sab.nl | |
| **D3. Do we provide a service to the client where we assist in providing copies of data if the data subjects request a copy?** | ☒ **Yes** ☐ **No** | |
| **D4. If yes, how will copies of data be provided to a data subjects if they request a copy?** | Webbased portal mijn-sab.nl<br>Mail<br>Post | |

| | | |
|---|---|---|
| **D5. Do we provide a service to the client where we assist in providing copies of data in a portable format if requested by the data subjects?** | ☒ **Yes** ☐ **No** | |
| **D6. If yes, how will copies of data be made available to data subjects in a portable form if requested?** | CSV file | |
| **D7. Has the data controller compiled a record for this processing which contains: purpose of processing, types of data collected, third parties to whom this data may be disclosed and data retention policy?** | ☒ **Yes** ☐ **No**<br>**If yes,** how has SAB checked/controlled this:<br>See processing register SAB | |
| **E. Security** | | |
| **E1. Security Officers in charge** | **Security Officers involved,**<br><br>**For Pharox if any :**<br>☒ **In GBU/Country,**<br>please specify the contact name:<br>☒ **In Project,**<br>please specify the contact name:<br><br>**For the customer if any :**<br>please specify the contact name: | Joël Grevelink (Security Officer Conxillium Group B.V,) Pharox Automatisering B.V. is part of Conxillium Group_ |

| | | |
|---|---|---|
| **E2. What are the relevant security measures in place (ISO 27001, ISAE3402, PCI/DSS, ….)?** | | • ISO 27001 certification for data center hosting service provider<br>• ISO 27001 and NEN7510 certification for system management provider |
| **E3. Physical access control measures** | | • The servers are operated on a secured data center, incl. air conditioning, alarm systems (heat, smoke), CO2 fire extinguishers (waterless), overvoltage protection, uninterruptible power supply (UPS), raised floor, protecting doors, redundancy of communications links etc.<br>• The secured data center for the website hosting is using Cisco firewall technology for the protection against hacking, malicious software etc.<br>• The servers are stored within secured and separate server racks. These racks are stored within separate and secured rack rooms.<br>• Access to server rooms only possible via secured data center. Only Pharox designated |

| | | |
|---|---|---|
| | | personnel have access to the data center. |
| **E4. Logical access control measures** | | • Direct access to servers only possible from Pharox office (IP address restriction via Secure VPN connection)<br>• All external access to the servers only possible via standard web browsers through firewalls and web servers<br>• External access to the system only possible via strong username and passwords |
| **E5. Logical application access control measures** | | • The authentication and access control on application level is realized to ensure effective protection and user specific information against unauthorized access. The authentication and access control is based on Oracle database security technology. The users' access rights for the websites are based on a predefined role concept and a dedicated support and maintenance account with just the access rights necessary. |

| | | |
|---|---|---|
| | | • Secure Log-in / password handling<br>• The users have no access to the server operating system. The users login via their web browser to a website application (and have the option to log-out again). Temporary user sessions, a timeout will lead to an automatic logout of the user.<br>• The user accounts are individual for each user, user accounts without passwords do not exist. The passwords which are entered, are concealed / not shown in plain text on the screen. The user management process is logged in the system.<br>• Password expiration policy in place |
| **E6. Disclosure control measures** | | • HTTPS (Secure HTTP) implementation to prevent inadvertent disclosure of data<br>• Access only possible via strong username and passwords<br>• Password expiration policy in place |

| | | |
|---|---|---|
| | | • Temporary user sessions, a timeout will lead to an automatic logout of the user. |
| **E7. Input control measures** | | • Input and modifcations are logged. There are log files created by the operating system, database software and application. The access to the logs is restricted to the system and application administrators. The logs are periodically checked.<br>• Monitoring system / application access and use |
| **E8. Separation control measures** | | Segregation of the application data is controlled by Oracle database security technology (via separate Oracle database schemas and database tables). |
| **E9. If sensitive data is processed, please indicate which specific security measures are implemented, if any** | | No specific security measures regarding sensitive data (if any) are implemented |

| | | |
|---|---|---|
| **E10. In case of transfer of sensitive data outside the EU, please indicate which specific security measures in place** | | Not applicable |

**Table 4 Details and DPO and DPLE comments / corrective measures**

# 4 Remarks and Further Applicable Documents

## 4.1 Remarks

Not applicable

# 5 Appendix

Not applicable