Data Handling Processes (Summary)

Document Details

Description

This document covers the general procedures required in the handling of data provided by a client ('client data') during the initial purchase of a product from Esferico ltd. and additional storage and processing of data thereafter.

The processing products in use are usually software based tools for the administration of client organisations – the most common form at time of writing being in Library and Information Management.

Detailed data handling processes are included in various internally manuals. This document should be regarded as a top level summary for both staff and client information.

History

Effective date of this document: 14th February 2018

Document Owner: Esferico ltd.

Version	Date	Description	Author
1.0	2018-02-14	Initial author	ESF-CR
1.1	2021-03-21	Replaced VPT with CR as DPO.	ESF-CR

Data Types

Client data typically consists of three different categories of data:

- General data regarding an inorganic item ('non-personal data') such as a book, video or other form of media artifact.
- Personal records identifying the data required to administer the client organization ('personal data') core functionality.
- Functional meta-data ('functional data') linking personal data with non-personal data, recording an operation or task undertaken by the client organization.

Functional meta-data within the Esferico ltd. product suite should always be designed and implemented in the form of internal database unique IDs linking to non-personal and personal data records. Functional data should not and cannot in itself therefore be utilized to identify an individual without the additional presence of personal data records.

Functional meta-data is therefore not considered within this document to be ‘personal data’, but it should always be remembered that [arguably] under the terms of the GDPR this data may be considered personal with the addition of linked personal-data records.

Regardless of these distinctions therefore, all three forms of data, if provided by a client, will be handled in the same way – privacy and security should err on the side of caution in case of data mixing, compositing or reconstruction during the data processing exercise.

Encryption

From 25th May 2018, all data transfers of personal data to and from Esferico ltd. should preferably be performed using the encryption tools provided by Esferico ltd. through the licensed products.

The reasons for this preference are:

- The Esferico ltd. encryption tool requests an unlock key from the user (e.g. the client) but which comprises only half of a two-part unlock key.
- The second half of the unlock key is generated by the Esferico ltd. software and is unknown to the client. The client should provide their unlock key to Esferico ltd. by a secondary route, but even if intercepted this unlock key will not decrypt the transferred data – this can only be done by reciprocal software within Esferico ltd. which is able to regenerate the Esferico ltd. half of the key.
- Licensed Esferico ltd. software is able to transfer the encrypted file directly to the Esferico ltd. server, secure it and make the file known to Esferico ltd. staff for download. This is the preferred data transfer method.

In the case of cloud-based applications, data to be transferred for processing should be uploaded directly to the cloud application using standard user authentication processes. Where possible all data proccesing should take place within the encrypted cloud application only, and not be transferred to local Esferico ltd. workstations.

Initial Data Acquisition

All client data acquired by Esferico ltd. for initial data import purposes is acquired only with direct involvement of the client, and only with prior arrangement through the purchase order and purchase details document provided to the client by Esferico ltd. Itself.

No client data is therefore acquired by Esferico ltd. having been initiated by the actions of the company – all client data transfer to Esferico ltd. is initiated by the client.

The following important points should be made known to the client by the member of Esferico ltd. staff involved in the transfer, preferably in writing or having been directed to this document stored online at the Esferico ltd. website, and data transfer should not begin until the client has confirmed Esferico ltd. as an authorized third-part data processor.

- From 25th May 2018, all personal data supplied to Esferico ltd. for processing must be provided by the client in a secure manner. At the very least, this should be in an encrypted format with unlock keys provided by separate, alternate routes. A mechanism for direct upload to secure Esferico ltd. servers will be made available for clients wishing to utilise this facility.
- Any and all personal data supplied to Esferico ltd. in a non-secure manner will be deleted immediately from both the communication method (e.g. email) and Esferico ltd. servers and will not be examined.

Data Processing and Storage During Processing

Data processing, especially where custom conversion utilities are required to be developed by Esferico ltd. requires readily accessible access to the client data. For this reason, data may remain on developer workstations but all developer workstations must be routinely secured following internal workstation guidelines (see separate document), including storage media encryption and user account based access.

Storage of data during processing, especially as the client data may additionally need to be accessible for a development team rather than an individual, should only be undertaken using the encrypted online drive configured for this purpose (see separate internal GDRP compliance and security documentation for more details).

Delivery of Processed Data

Delivery of processed client data should be performed at least at the same level of security as original delivery to Esferico ltd. specifically:

- All processed data supplied to clients by Esferico ltd. from 25th May 2018, will be supplied in an encrypted format with an unlock key provided by an alternate route.
- To provide a second level of security, data supplied in this manner will only be available for direct download from the secure Esferico ltd. servers, using a pre-authorised user account protected by SSL/TSL, for a short duration of time which will then be revoked.
- From 25th May 2018, no data will be provided to clients by email attachment.
- Where data is to be used within a cloud application, all data should be uploaded to the application from secure Esferico ltd. workstations and then provided to client access only via the cloud application account authentication systems. All databases are to be secured with highest level real-time encryption systems available.

Long Term Data Storage

Long term data storage is intended to balance a responsibility to provide technical support, remain secure but also coupled with the responsibility to provide suitable data backup and restore options.

As part of this multi-level responsibility:

- On 25th May 2018, all currently archived processed personal data stored for support purposes will be permanently and irrecoverably obfuscated on the Esferico ltd. servers. From that point on, it cannot be utilised for support work which relies upon the identification of individuals and the data may be regarded as now being 'non-personal data'.
- All future processed data (conversions delivered post 25th May 2018) will be stored only for 1 (one) calendar month in the original format to allow for initial conversion support following installation, and then all personal data will be similarly permanently and irrecoverably obfuscated and may be regarded as being 'nonpersonal data'. Given the impracticalities of deletion and/or pseudonominisation of individual records in archives stored only for support purposes, this is the only safe GDPR compliance option available.
- All processed client data in its obfuscated format will be stored on the central encrypted secure storage environment, additionally pre-encrypted at the database file level, as well as the local Esferico ltd. servers acting as a local mirror. All local servers are encrypted at a file-system level, as well as requiring authorised user account access.

Ongoing Support Regarding Access to Personal Data

As far as is possible, support of end-clients should be performed without the need to access personal data. This is especially true as current Esferico ltd. policy is for 1st line procedural support to be administered by local authorised agencies (such as local School Library Services, for school libraries).

GDPR relationships between the client and the said authorised agency is therefore outside the control of Esferico ltd.

On occasion however, it may be necessary to access a local database. For this purpose, two options are permissible:

- Authorised and observed access to the local database environment / installed software using a secure remote access tool, if permitted by the client, such as Microsoft RDP or TeamViewer. Access should not be attempted without the presence of a local member of staff.
- If the transfer of the database is required to Esferico ltd. such as for more detailed investigation using internal support tools, the transfer of personal data to Esferico ltd. will only be undertaken following local anonymisation of that data using the utilities provided by Esferico ltd. within the licensed software product (see Reader Obfustication). No live personal data should be transferred to or from Esferico ltd. in a non-encrypted or non-anonymised form.

All data transfers should be undertaken using a pre-encrypted database with the unlock key transferred using a separate route. The encrypted database should be preferably transferred directly to the Esferico ltd. secure server using a temporarily available secure user account, or in the case of a cloud application using the application's standard user account authentication processes.

Support of cloud-based applications, the preferred method of application support, should only be performed using the available secure user authentication systems of the application.

GDPR Roles and Employees

Esferico ltd. have designated Craig Robinson as our Data Protection Officer (DPO) and have appointed a data privacy team to develop and implement our roadmap for complying with the new data protection Regulation. The team are responsible for promoting awareness of the GDPR across the organisation, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures.

Esferico ltd. understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have involved our employees in our preparation plans. The procedures listed in this document are made available to all Esferico ltd. staff through an ongoing training and reminder program and everyday implementation is accompanied by a checklist based system to record compliance.

If you have any questions about the procedures described in this document, please contact Esferico ltd. in writing at dpo@esferico.net