30-11-2015

Milestone MNA3.2: Requirements on data to protect from AAI, community, resource providers and e-infrastructure

Milestone MNA3.2

Contractual Date:	30-11-2015
Actual Date:	30-11-
Grant Agreement No.:	653965
Work Package:	NA3
Task Item:	TNA3.5
Lead Partner:	KIT
Document Code:	MNA3.2
Authors:	Uros Stevanovic, David Kelsey, Ian Neilson, Gerben Venekamp, Ramon Bastiaans, Jules Wolfrat, Walter de Jong, Petr Zabicka, Melanie Imming, David Groep, Marcus Hardt, Mikael Linden

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

Abstract

Communities of researchers and students, as well as the research and computing and data infrastructures, need to be able to process data and meta-data about the users and their interaction with the systems. This is essential for accounting and for assigning use data to allocations, and to be able to follow up on incidents in the infrastructure. Before recommendation can be developed, it is necessary to make an inventory of the relevant use cases, identify the types of data generated within the infrastructure as a result of its use, and the respective roles of the participants in the infrastructure with respect to data protection. This document provides this basis for further recommendations.

Table of Contents

Executive Summary

In the first phase, this task will provide an overview of requirements and template policies for the processing of personal data for each of the identified participants. The ultimate aim will be to provide recommendations that can be applied across the entire infrastructure – bearing in mind the current state of European legislative efforts and the implementation thereof in the member states. It will identify the minimal set of information needed by the participants in the prevalent use cases and those foreseen for the proof-of-concepts in SA1. The scope of the task will be limited to the collection and processing of personal data from user communities and infrastructures (as suppliers or associations), and will not cover the policies for attribute release.

Collaborations between different administrative domains and across borders in Europe and beyond need to address the management of personal information. Most of the research use cases, and all of the cross-domain resource providers and e-infrastructures, will have to process such data in order to measure usage and allocate resources. This data needs to be protected and, at the same time, be made available to those who have a legitimate reason to view and process it.

1 Introduction

The purpose of this document is to collect input and requirements that will form the basis for development of specific recommendations and template policies to sites and user-communities so that they will be able to collect, transfer, provide access to and/or publish data related to the following categories: Accounting, Monitoring, and Logging. Questions related to attribute release or how security incidents should be handled given the available data are not in the scope of this task.

This document presents:

- requirements from the communities illustrated by example use-cases
- categories of data to assist in making decisions about how these data should be handled
- existing legal privacy frameworks from European and national bodies
- existing policies of communities and infrastructure providers regarding collection and processing of personal data

2 Requirements

This chapter examines common use cases for collection and processing of personal data from the point of view of two distinct infrastructure providers and a typical user community by describing the following for each of these cases:

- The purpose and reasons for the collection and storage of the information
- Control of and access rights to the information
- The period of retention
- Publication of the information
- Protection of the information
- Access by the user to their own information

2.1 Infrastructure providers

2.1.1 EGI

EGI is an example of a general purpose infrastructure provider serving multiple user communities.

2.1.1.1 *The purpose and reasons for the collection and storage of the information*

Information collection and storage is conducted for Virtual Organizations (VOs[1]) to plan, monitor and control their resource allocation. Sites conduct monitoring to discern how the resources they provide to the Infrastructure are being used and by whom. Infrastructure management or VOs need to detect whether resources committed were indeed provided and properly used. VOs, Infrastructure Management and Sites need to report on usage to their respective funding bodies. User-level accounting is used to determine how the resources within the VO, group or role are being used. Anonymised and aggregated statistics are provided to

[1] Virtual Organization is a grouping of users and optionally resources, often not bound to a single institution, who, by reason of their common membership and in sharing a common goal, are given authority to use a set of resources.

funding bodies and are used for operational and scientific analysis. Infrastructure Operations use user-level accounting for troubleshooting and debugging. Finally, Security Operations use accounting, monitoring and logging data in investigation and containment of security incidents. Here, the aim is to retain all relevant information, including timestamps and digital identities of the users, sufficient be able to answer the basic questions who, what, where, when and how concerning any incident.

2.1.1.2 *Control of and access rights to the information*

The local accounting record for a job is controlled by the site at which the job is executed. The submitting user's identifier (the Distinguished Name field in their X.509 certificate - DN) may be unencrypted in this information and access is restricted to the local resource administrators or other authorised persons. Each site is responsible for sending its accounting records on a regular basis, with at least user DNs securely transported, to a central data base defined by the Infrastructure. This database is located at an Accounting Data Centre (ADC), whose location needs to be chosen carefully according to data privacy laws. Copies of individual job accounting records and aggregated data in the ADC central database are controlled by the Infrastructure. Only ADC staff may be authorized to have access to individual job records, according to their role or job responsibilities. Access to aggregated data at the VO level may be public information if the VO agrees, while access to VO group/role aggregated data is restricted to members of that VO. The aggregated data of a user must be properly protected. All user data in the database are anonymous in the sense that the user data cannot be connected to a user name. Access to this anonymised data, if requested by the VO, must be restricted to members of that VO. Connecting the pseudonymised name with a person's DN is restricted to individuals in the VO appointed to be VO Resource Managers.

2.1.1.3 *The period of retention*

Sites are responsible for storing the local accounting records long enough to ensure their successful transfer to the ADC database. Afterwards, they can be deleted in accordance with local personal data retention policy. The ADC is responsible for deleting the copies of the individual accounting records in the central database, or for removing or anonymising personal identifying information.

2.1.1.4 *Publication of the information*

The ADC publishes accounting data on its web portal for which appropriate access control must be agreed between the Infrastructure and the VO. The ADC publishes user-level accounting data to authorised VO Resource Managers, if requested by the VO.

2.1.1.5 *Protection of the information*

The Site managers and resource administrators are responsible for the secure storage of the local accounting data, and appropriate access control mechanisms need to be in place to prevent unauthorized access. The ADC must implement appropriate technical and organisational measures to protect the accounting database and the accounting web portal.

2.1.1.6 *Access by the user to their own information*

A user has a right to view their own accounting records, and mechanisms for a user to access their own aggregated user information must be implemented. It must also be possible to correct that data if the user can prove that the stored data is wrong.

2.1.2 PRACE

2.1.2.1 *The purpose and reasons for the collection and storage of information*

Information on the usage of resources is stored by PRACE sites in the first place to control the amount of resources which are assigned to PRACE projects as a result of the PRACE Peer Review process (PRACE Peer Review) or to DECI projects (DECI projects). In addition this information can be employed by users to monitor their usage of resources and by principal Investigators to monitor the usage of their projects. Summarized information is used for management reporting, e.g. to control the commitments of the total PRACE resources by partners.

For DECI projects some sites export summary information to a central database. This database is primarily used to provide information for users and Principal Investigators.

Information about access to resources by users is logged by sites and can be used in case of security incidents.

Contact information about users is stored in local site databases and sometimes also in a central database.

2.1.2.2 *Protection of the information*

The sites are responsible to protect the data from unauthorized access and to define and control the access rights. If the data is exported, the site hosting the imported data must have implemented agreed access controls and protect the data from unauthorized access.

2.1.2.3 *Control of and access rights to the information*

There are currently four access levels or roles defined:

- End user, who only has access to his/her own usage records and contact information
- Principal Investigator, who has access to specific project records and his/her own personal information
- Site staff, who have access to local records or remote records if needed.
- Management, access to information through summaries.

Local access to the information at sites is provided through site dependent facilities, in principle based on local identity information. In principle all user accounts are unique and may not be shared.

Remote access to accounting records can also be provided by sites through a web service using X.509 certificate based access control. The above defined roles are used to control the access rights. Only data to which the user should have access is exported from the site. Access to the central accounting database is also controlled based on the roles defined above. In this case only summary information (currently on a monthly basis) can be provided. Site staff has access to the central user database with defined read and write permissions.

2.1.2.4 *The period of retention*

The period of retention of the data depends on site policies and national regulations. The web based accounting information is expected to be at least accessible for a period of one year after the end of the project. Personal data should be removed following EU and national regulations. Only the information that can guarantee that accounts will not be reused for different entities must be kept, e.g. the login name cannot not be recycled.

2.1.2.5 *Publication of the information*

Only high level information about projects and users is published, e.g. total consumed resources of a project and information about users who worked on a project. Accounting information is only accessible for authorized entities. Other stored data only will be shared within the infrastructure with site staff if needed. Sharing of data with other infrastructures will only be possible if there is some form of agreement, e.g. a MoU or contract, and accepted by the user.

2.2 Community infrastructure

2.2.1 DARIAH

DARIAH is chosen as an example to explain requirements and policies common for a community infrastructure.

2.2.1.1 *The purpose and reasons for the collection and storage of the information*

DARIAH collects information for monitoring purposes. Manual bug tracking is conducted when a signal of failure comes from the user. Furthermore, the community Identity Provider availability is monitored, as well that of some key Service Providers. This includes monitoring LDAP, virtual machines, CPU and disk usage, etc. The Community LDAP-Server, which is managed via Web-based SelfService and Administration portal, is also monitored. There are policies which inform the user about the user accounting data: Privacy Policy for DARIAH Services and Terms of Use (in german).

Types of data which are collected:

- Bug tracking information is currently not anonymized, but anonymization is implemented and will be put in place shortly. Processing of the data involves manual introspection and checking log files.

- Monitoring data do not contain any personal identifiable information. For monitoring icinga/Nagios is used. Data are collected every 5-60 minutes for Nagios. Accounting data are organized per host, or per service.

- LDAP server contains personal data on users (homeless as well as those authenticating via their Home IdP).

Use cases for which data are collected: bug tracking, monitoring.

2.2.1.2 *Control of and access rights to the information*

Policies exist which define who has access to the accounting data. Access to the information is only available to dedicated admins. For bug tracking, only local admins have access. Parts of the monitoring data are public, while some of the data are available only to admins on a federated level. LDAP server accounting data are accessible only to responsible admins (decentralized).

2.2.1.3 *The period of retention*

Bug reports are stored until the resolution of the issues, afterwards the data are to be removed. User data are being deactivated and later deleted by automated processes that react on email delivery failures and manually upon request.There is no policy in place for deleting monitoring data, since they do not contain personal data.

2.2.1.4 *Publication of the information*

Information about the bug reports coming from users are not published, and are only accessible to responsible persons (admins). Usage statistics and monitoring data are partially published, however, this data does not contain any personal information. The overall status is published to funding bodies.

3 Types of Data

Types of personal data collected can be sorted on three levels: personal, group, and public. Also, additional types of data exist, such as data about operations.

3.1 Personal data

Personal data are any kind of information that can be used to identify an individual. Personal data could be further categorised into identifiable, pseudonymised, and anonymous with each having different legal ramifications.

3.1.1 Personal identifiable data

Identifiable data are any information relating to a user (identifiable natural person), and their physical, physiological, mental, economic, cultural or social identity. This includes IP address of a user, phone number, address, personal or username, its aforementioned identities (e.g. social, cultural), gender, age, email address (non-exhaustive list).

Regarding general service providers or community infrastructures, different data elements and different amounts of data are collected. In the case of EGI for example, the personal data that each user provides is:

- Family and given name
- Institute name
- Contact phone number
- Email address
- Distinguished Name (DN) extracted from a valid personal digital certificate

EGI also collects Infrastructure operations logs of every executed individual job. These logs contain identifiable information such as usernames and timestamps. This provides the minimum level of traceability for Infrastructure usage to be able to identify the source of all actions (executables, file transfers, pilot jobs, portal jobs, etc) together with the individual who initiated them.

In the example of community infrastructure, DARIAH, the amount of collected data is not so extensive. Usually the login logs (indication if the user has logged or not) and, when the need arises, manual bug reports are collected. These data contain information about the user i.e. username and email.

Legal policies exist which regulate the collection, storage, and protection of personal data. For the collection of personal data, usually the user must consent to its collection. Exceptions do exist, when there is a legitimate interest in collecting personal user data. Also, measures need to be implemented to ensure the safety and reliability of the data collection and storage.

3.1.2 Personal pseudonymised data

Personal pseudonymised data differ from the identifiable data in the sense that instead of the collection of the actual username, each user is assigned a unique identifier. Since, in general, a mechanism exists where the identifier can be connected to the actual user, the same legal and site policies are valid here as for the personal identifiable data. Personal data must be secure, and accessible only to authorized persons. Users must give consent, or there must exist a legitimate reasons for the collection of personal data.

3.1.3 Personal anonymised data

Anonymised personal data do not contain any information which can point to the identity of a user (e.g. no IP address information, nor username, email, etc.). As such, the user’s consent for its collection, processing, publication is not necessary. However, informing the user of the existence of such processing is recommended. Also, legal policies for personal data do not consider the need for protection or restriction of such data, and defining the usage and types of processing is left to the service provider infrastructures and communities.

3.2 Group data

Group data, where data are collected at the level higher than at which an individual user can be identified, do not contain any personal identifiable information. Typical examples include CPU usage and storage occupancy. As the user's identity is not discernible, the same recommendations and policies apply as for the fully anonymised data.

In some cases it is difficult or impossible to anonymise group data. For example, if a group consists of very few users, an additional criterion (e.g. country where logins came from) may be used to identify (i.e. de-anonymise) a user. Such data is not anonymised. In this instance a care must be taken to avoid conflict with privacy policies.

3.3 Public data

Public data are collected for the purpose of publishing the usage of the resources provided by the infrastructures. They may include, but are not limited to, CPU usage, RAM, storage, uptime, number of executed jobs, etc. Usually, they are automatically collected and generated using e.g. Nagios/Icinga

4 Policies

4.1 Legal Policies

This chapter will provide existing legal framework in processing user data. The scope will cover both European and national legal policies. For legal policies, the key document is Directive 95/46/EC which regulates the duties and roles of various parties. For example, resource centres and e-infrastructures have a role as a supplier, in which they deliver services, and they can do processing of personal data based on the grounds of legitimate interest (art. 7(f)). Since for the purpose of using resources provided by the centres and e-infrastructure, data subjects are "customers", and as such, for as long as there are legitimate reasons to collect and process data, processing can continue. This also applies to the disclosure of data to third parties, if the legitimate interest exists.

4.1.1 European legal policy

The protection of individuals with regards to the processing of personal data and the free movement of such data is regulated with the establishment of Directive 95/46/EC. The document is not legally binding, however it is meant to be a starting point from which all member states should implement their own data protection policies.

The Directive identifies following terms:

- **personal data** as "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"

- **processing of personal data** as "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".

- **Data controller** means "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law".

- **Data processor** means a "natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".

- **Third party** means “any natural or legal person different than the one data processed is concerned about”.

- **Processing** means “any operation or number of operations with or without use of electronic data processing to which the data are subjected”.

For the processing of personal data, the Directive applies “only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question”. For the processing of data “which are capable by their nature of infringing fundamental freedom or privacy” a user must freely give their explicit consent. Exceptions do exist, such as for health-related purposes and in the course of pursuing legitimate interest and activities.

Important principles:

- **Identification of personal data** - According to Article 8 section 7: “Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed”.

- **Information presented to the data subject**: This refers to information that has to be presented to the subject when collecting and processing his/her personal data. Article 10 describes the minimum information needed to ensure transparency to the subject: (a) the identity of the controller and his representative, if any; (b) the purposes of the processing for which the data are intended.

- **Right of access**: Article 12 states that there should be a high level of transparency between subject and the controller. In short, the following should be provided: confirmation of data processing; recipients to which data might be disclosed; knowledge of processing logic of data; ability to rectify, erase or block data if it does not comply with the provisions of the Directive.

- **Confidentiality** According to Article 16: “Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.”

- **Security of processing** - According to Article 17, Section 1: “Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. With regards to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

  Section 2: “The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures”.

> Section 3: “The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller”.

The regulations in this directive outline general principles about personal data protection in the EU. Largely, the principles state that security and confidentiality should be implemented according to a risk assessment of the system that handles data processing, while taking into account a certain level of transparency to the data subject regarding his/her personal data. In terms of data transferred between member states and countries outside the EU, the Directive states that all parties should ensure compliance with the policies stipulated in the document.

In January 2012, a new proposal for a General Data Protection Legislation was issued by the EU Parliament. This new document aims to add and enforce some key concepts from the previous directive such as: guaranteeing easy access to one’s own data, right to be forgotten (deletion of data), explicitly given consent for processing data, ensuring a single set of rules for all member states, and clear rules for data controllers outside the EU.

4.2 Resource infrastructure policies

In case of EGI, there are several documents which outline the policies for traceability, incident response, personal data collection and processing, etc.:

- Job accounting data policy presents the minimum requirements and policy framework for the handling of user-level accounting data created, stored, transmitted, processed and analysed as a result of the execution of jobs on the Infrastructure.

- Grid Acceptable Use Policy describes the conditions that have to be accepted by all Users during their registration as a user of the Infrastructure.

- Grid Security Traceability and Logging Policy defines the minimum requirements for traceability of actions on Infrastructure Resources and Services as well as the production and retention of security related logging in the Infrastructure.

- Virtual Organisation Membership Management Policy defines the minimum requirements on Virtual Organisation (VO) Managers for managing the members of their VOs. Document also states which data are supplied by the user.

For DARIAH, as previously mentioned, the main documents which inform the user about policies are:

- Privacy Policy for DARIAH Services

- Terms of Use (in German)

4.3 Policy regarding exchange of incident data

The handling of security incidents may require the exchange of information where the relationship between the exchanging parties is not necessarily pre-defined by Federation, Memoranda of Understanding, common policy sets or other such agreement. A simple example, but by no means the only circumstance, is the compromise by loss of password or other authenticator of a researcher's account at one federation resource provider where the researcher participates in multiple such infrastructures. How should this knowledge be communicated between federation resource providers when they have no agreement or established trust relationship? In such cases the objective of exchange is to protect the integrity of the infrastructures. This may be via passing relevant information about internal events to third parties to assist in closure and full understanding of the extent of an incident, or conversely by receipt of information to allow, for instance, the proactive investigation and protection of the infrastructure before external events propagate across operational boundaries.

Whilst the legal frameworks may acknowledge this use case, they are not explicit in policy terms as to how to satisfy the requirements on the exchange. Clearly the sending party should trust the receiver to treat exchanged information, which may contain personal identifiers, appropriately. The SIRTFI group, a REFEDS working group, is looking at processes for expressing security incident handling requirements as an assurance profile for federations and other requirements needed to effectively deploy and enhance incident response processes for Federated Identity Management.

The SIRTFI Trust Framework specification, which defines basic security incident response capabilities to which member organizations can self-assert compliance, is currently (November 2015) released as a consultation document. When finalised, the group may begin the process of taking the paper forward as an Internet Draft and towards an RFC. If successful, and with an associated technical standardisation of the exchange of incident response contact meta-data, incident handlers should have a framework within which incident data can be exchanged with assurance that the information will always be protected and managed appropriately.

5 Summary

The Milestone sets the scene for the Deliverable D3.5, due in Month 18. The document lists requirements, legal and resource centres policies regarding storing and processing personal data, and which types of personal data are collected. The requirements, policies and types of data which are presented here will serve as inputs for SA1.

Appendix A National legal policies

A.1 German legal policies

One of the most important laws regarding user data is Federal Data Protection Act (Bundesdatenschutzgesetz, or BDSG), which serves to implement the Directive 95/46/EC. The purpose of the act is to protect the individual against his/her right to privacy being impaired through the handling of his/her personal data. The second important law is Telemedia Act (Telemediengesetz, or TMG).

Important aspects of BDSG law are:

- **Personal data** - This is any information concerning the personal or material circumstances of an identified individual. Special categories of personal data includes information on a person's racial/ethnic origin, political opinions, etc. (S. 3.1,9)

- **Data collection** - Collection of personal data is allowed only if stipulated by law or if the user has explicitly consented (S. 4.1). Personal data are to be collected, processed and used as little as possible (S. 3a). When the personal data are collected, controller (meaning any person or body which collects the data) needs to inform the user of the identity of the controller, the purpose of the collection and, if needed, the recipients to whom the data will be transfered (S. 4). User must consent for the collection of data, in writing (S. 4a.1), however, for scientific research the consent doesn't have to be in writing if that would "impair the purpose of the research considerably" (S. 4a.2).

- **Data processing** - From Section 3.4 and 3.5: "Processing" means the storage, modification, transfer, blocking and erasure of personal data. In particular cases, irrespective of the procedures applied: "storage" means the entry, recording or preservation of personal data on a storage medium so that they can be processed or used again, "modification" means the alteration of the substance of stored personal data, "transfer" means the disclosure to a third party of personal data stored or obtained by means of data processing either through transmission of the data to the third party or through the third party inspecting or retrieving data held ready for inspection or retrieval, blocking" means labelling stored personal data so as to restrict their further processing or use, "erasure" means the deletion of stored personal data. "Use" means any utilization of personal data other than process. Automatic data processing procedures needs to be registered with the competent supervisory authorities, unless there is a data protection official. (Section 4d).

- **Transfer of personal data** - Transfer of personal data between bodies within the European Union, states within the European Economic Area, or bodies of the European Communities is permissible with activities which fall in part or in their entirety within the scope of the law of the European Communities (Section 4b). Transfer to other bodies (outside of European Communities) is not permissible if the level of the data protection is not adequate, or if the data subject has a legitimate interest in excluding transfer.

- Right of access - The data subject has a right of access to its personal data, and also has a right to correction, erasure and blocking of personal data (Section 6). In case there are several bodies which store the subjects personal data, the subject may approach any of them, and the contacted body must forward the request to the body which has stored the data. Also, personal data are to be erased if their storage is no longer needed for processing. However, in case if erasure is not possible or is only possible with disproportionate effort due to the specific type of storage, in such case personal data will be blocked (section 20).

The BDSG also mentions the compensation if processing of personal data causes harm to the data subject.

The TMG scope of application is for all communication services and electronic information, unless it is involved in transmission of signals in the telecommunication networks. Service providers shall be responsible for their own information which they keep ready for use, in accordance with general legislation. Also, they are not required to monitor the information transmitted or stored by them or to search for circumstances indicating illegal activity (Section 7). The service providers are not responsible for the information of the third parties if they have not initiated the transfer, selected the address, modified the information, nor stored no longer than it is needed. Also, the service providers are not responsible if they act expeditiously to remove the information upon obtaining knowledge that it is involved in illegal activity (Sections 8-10). User must be informed of the collection and use of the personal data, which can be stated electronically, if the recipient has given it consciously and unambiguously, if the record of it is kept, and the user can access it and revoke at any time (Section 13). Furthermore, the TMG act also defines fines (monetary penalties) for certain behaviours.

A.2 Dutch legal policies

The Directive 95/46/EC is translated into Dutch Law (Wet bescherming persoonsgegevens) and is expected to be replaced by a new European regulation in 2017. The purpose is to protect the privacy of individuals. It states what is and what is not allowed with personal data and the rights an individual had. It states that individuals have a right to information, review its data and to resist usage of its data. Specifically it regulates the following:

- **Obligatory information on personal data** - Registering, use, forward one’s personal information by organisations requires that the owner is informed. In case of executing legal duty by organisations, informing the owner is not required.

- **Right to review and correction of personal data** - Written request to organisations in order to view stored personal data. The organisation is required to give a written response within four weeks. In case of inconsistencies in the data the organization is obligated to correct those. In case of offenses or to protect the rights of others, an organisation is allowed deny the request.

- **Right to motivation** - An organisation must be able to motivate why a service is denied.
- **Privacy data for marketing purposes** - Objection to the usage of personal information for the use of marketing purpose. Personal data must be removed from databases with a minimum of anonymisation.
- **Personal data processing by the government** - Governments must have policies to protect personal data from being transferred to organisation outside the government. An individual has the right to ask its government not to share its data with other organisations.
- **Submit dispute** - In case of an organisation that is processing personal data and the data owner has an unresolvable conflict, it can consult College bescherming persoonsgegevens (CBP - Dutch only), or a judge.

See also this document (Dutch only).

A.3 British legal policies

In the UK the Information Commisioner's Office (ICO) is the responsible body for upholding information rights in the public interest including the UK Data Protection Act 1998 (DPA) which implements the Directive 95/46/EC of the European Parliament. The ICO publishes concise guidance for organisations regarding their obligations under the DPA.

A.4 Danish legal policies

In Denmark, data security and privacy are stipulated by the Act on Processing of Personal Data (the Act, or APPD for short) and the Executive Order on Security (EOS). The former aims to stipulate the processing of personal data for individual citizens in general. It is intended to be flexible and take into consideration the use of modern technologies. It implements EU's Directive on the protection of personal data. The Executive Order on Security is intended for the processing of personal data on behalf of the public administration. The Danish Data Protection Agency (Datatilsynet) is responsible for all processing operations covered in the act. The only exception is data carried out on behalf of the courts. This data is supervised by The Danish Court Administration. According to Section 58 of the Act, The Data Protection Agency shall supervise, on its own initiative or acting on a complaint from a data subject, that the processing is carried out in compliance with the provisions of this Act.

Important aspects are:

- **Security of processing data** - According to Section 41 of the Act, the controller or the processor shall implement appropriate technical and organizational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure. Moreover, Section 14 of the Executive Order on Security states that external communication connections may only be established if special measures are taken to ensure that unauthorized parties cannot gain access to personal data through these connections. In the Guidance to Executive Order no. 528 of 15 June 2000 on Security Measures for Protection of Personal Data, that is processed for the Public Administration, it is stated that in order to determine the security level, it is necessary for the controller to conduct a comprehensive risk assessment including all elements of the communication connection. Regarding cloud computing, propositions and ideas for the risk assessment may be found in ENISA's publication, "Cloud computing – Benefits, risks and recommendations for data security".

  Where a controller leaves the processing of data to a processor, Section 42 of the Act applies. In these scenarios, the controller shall make sure that the processor can implement the technical and organizational security measures, and shall ensure compliance with those measures. Furthermore, the Guidance to the Executive Order on Security states that the controller must actively ensure that the processor actually implements the required security measures and that it may be relevant to obtain an annual auditor's statement from an independent third party. The carrying out of processing by way of a processor must also be governed by a written contract between the parties (Section 42). The contract must state that the regulations in the Executive Order on Security also apply to the processing by the processor. If the latter is established in a member country, the processor must both comply with the Danish security requirements and the requirements in the processor's home country.

- **Transmission of data to third countries** - According to the Act on Processing of Personal Data, a third country is any state, which is not member of the European Community (EU/EEA) and has not implemented agreements corresponding to those laid down in Directive 95/46/EC. According to the law, a transfer to a third country may only take place if that country implements adequate security policy related to Directive 95/46/EC. It is also possible to transfer data if the person has given his/her consent explicitly (Section 27). Another possibility is if the data controller enters into an agreement based on the EU Commission's standard contractual clauses with the data centers in the third countries which will ensure that the data controller provides sufficient guarantees for protection of the rights of those registered.

- **Notification of data processing** - The Act on Processing of Personal Data contains a principal rule, stating that the Danish Data Protection Agency must be notified before processing of personal data is executed. In relation to the notification the Danish Data Protection Agency must issue an authorization or a statement before the processing (Sections 48-51). The notification should contain information about the controller and details about the processing itself. Furthermore, the duty of notification lies with the data controller.

- **Deletion of personal data** - Regarding the deletion of personal data, the guidance of the Danish Data Protection Agency to Section 9 of the Executive Order on Security states that when discarding or removing the data, the storage media needs to be destroyed, or demagnetized, or overwritten with the use of a special program which overwrites several times (e.g. DOD 5220.22-M). Moreover, according to Section 5 in the Act, the collected data may not be kept in a form which makes it possible to identify the data subject for a longer period than is necessary for the purposes for which the data are processed.

- **Control of rejected attempts to access data** - Section 18 of the Executive Order states that all rejected attempts to access data must be registered. Besides that, a comprehensive security mechanism must be implemented. This mechanism should ensure that if a predetermined number of consecutive failed login attempts are registered from the same workstation or with the same user identification, further login attempts must be blocked. Basically, the system should observe the access attempts and react properly if a pattern of incorrect attempts is observed. This reaction may be to close the user identification used, or to shutdown the PC or access to the local network. Furthermore, the reaction must be of such a nature that the event comes to the knowledge of the right person, i.e. system administration.

- **Logging** - Another important provision in the Executive Order states that all use of personal data must be logged (Section 19). Section 19 provides a list of details, which at least should be contained in the log – the time, user, type of use and an indication of the person the utilized data referred to, or the search criterion used. Furthermore, there is a restriction on the period of time the log can be kept for. By default this period is six months and after that the log must be deleted. However, authorities with special needs may store the log for maximum five years. Also, there are some exceptions for which logging is not necessary.

References

All references are embedded as hyperlinks in the text.

Glossary

REFEDS	Research and Education Federations group
SIRTFI	Security Incident Response Trust framework for Federated Identity
VO	Virtual Organisation – a user community, optionally with its associated resources