THE OFFICE OF THE DATA PROTECTION OMBUDSMAN

PREPARE A DATA BALANCE SHEET

24.4.2012

CONTENTS

1. WHAT IS A DATA BALANCE SHEET

Financial statements have a long history as a form of reporting the financial status of an organization. Financial statements reporting has also been extended to the different subareas of an organization's activities and its internal control and risk management. Other forms of reporting which supplement the financial statements are the sustainability reports and the statement of human resources prepared by companies and organizations. Extending the financial statement approach to information resources, information management, data processing and information security is naturally the next step in this development.

While the data balance sheet may supplement statutory reporting based on financial statements and annual reviews, the purpose is not to unduly add to the administrative burden of the organization. The data balance sheet is intended as a dynamic tool, which supports the efficiency, impact, and competitiveness of the organization.

The purpose of this guide is not to present an exhaustive formula or list of the information to be included in the data balance sheet. Its contents may vary, depending on the sector in which the organization operates and the nature of its operations. Therefore, it is advisable to introduce the data balance sheet to the extent to which it is expected to have a positive impact on the organization's operations.

The data balance sheet is an element of knowledge management and the organization may use it as an internal knowledge management report. The data balance sheet may also be used to report on key data processing issues to the organization's stakeholders. The data balance sheet is a report based on an internal review, which:

- provides an overview of the current status of data processing in the organization
- describes the information resources controlled by the organization
- describes the information flows related to the organization's operations
- describes the interoperability of the organization's information flows and data processing
- describes how data protection and information security are realized in the organization's operations
- describes the risk management procedures related to data processing
- supports planning and activities in the organization
- supports reporting and leadership in the organization
- serves as a follow-up tool for monitoring development measures
- serves as a tool for external stakeholder reporting
- ensures compliance with applicable legislation.

The principles of the Personal Data Act (including the duty of planning, duty of care and duty of protection) already address many of the issues to be included in the data balance sheet. The data balance sheet also complies with the principle of accountability, according to which an organization itself demonstrates its compliance with legislation and good practice in data processing and information management. In the future, data protection legislation may require the introduction of practices complying with the accountability principle. Before this happens, organizations may nevertheless proactively introduce the data balance sheet at any time. The documentation of issues during the data balance sheet process also guides towards a more systematic and critical review of issues.

2. WHY SHOULD AN ORGANIZATION PREPARE A DATA BALANCE SHEET

The high quality of data and efficient data processing procedures have a positive effect on all of the functions of an organization. Information is a valuable production factor, and the only one which increases strongly. New services are continuously being created around various kinds of information resources. These services are important for the success of the information society as a whole.

In the network and information society, data processing is of great significance to the realization of the rights and obligations of individuals and organizations. For instance, in its decision No. 20511/03, the European Court of Human Rights found that the Convention for the Protection of Human Rights and Fundamental Freedoms is also applicable to the assessment of the effects of data systems. In the public sector, data protection and information security have also become permanent elements of good governance. Data processing is also crucial to an organization's competitiveness, impact, and efficiency.

New services and electronic service processes necessitate the development of information structures and data management-related methods. This creates new challenges for the secure and responsible processing of data. Examples of new challenges include the purchasing and utilization of computing capacity and services via various cloud services. There is a need today for an across-the-board approach to information resource management. Preparing a data balance sheet offers a solution for such needs.

The data balance sheet describes compliance with the good data processing practices as referred to in the Personal Data Act. As regards public officials, the data balance sheet describes compliance with good practice in information management as referred to in section 18 of the Act on the Openness of Government Activities (621/1991). Good practice in information management requires that the availability, protection, and quality of the data are secured. The data balance sheet may be used to evaluate and promote the interoperability of information systems referred to in the Act on Information Management Governance in Public Administration (634/2011).
Experience shows that the data balance sheet is particularly useful in public administration organizations, the operations of which are based on the processing of extensive information resources and cooperation between controllers.

From the perspective of good data processing practice, the most important provisions of the **Personal Data Act** are the key principles of Chapter 2 of the Act:

- duty of care and lawfulness (section 5)
- predefined purpose of processing of personal data (section 6)
- exclusivity of purpose of processing and restrictions to the processing (sections 7 and 8)
- principles relating to data quality (section 9)

Chapter 7 of the Personal Data Act contains provisions on information security and the storage and protection of data.

Compliance with other legislation or information security standards may also be described in the data balance sheet.

2.1. The data balance sheet as an element of trust

Minimizing risks, building a good reputation, and retaining the trust of citizens and consumers are all issues increasingly important to success in all sectors. In order to promote these objectives and to gain competitive edge, responsible organizations use methods which support their activities and do more than what the minimum requirements in legislation require.

In a network environment in particular, inadequate data protection is regarded as a problem with regard to the trustworthiness and availability of the service. In the wrong hands, personal data poses a risk to the rights of the data subject (the person to whom the data pertains) and to the operations of the organization neglecting its responsibility for data protection.

The trust of customers and stakeholders in an organization's data protection and information security practices is an element which strongly supports the organization's operations. Observing data protection and information security in connection with online services, for instance, is a duty prescribed in law. It is also an essential element of good service.

The existence of a data balance sheet tells stakeholders that the organization considers it important to focus resources on data processing procedures and on compliance with good practice in data processing and information management.

2.2. The data balance sheet as a management tool

Integrating information management as part of the overall management of the organization is a major operational challenge. The executive management must have an overall idea of the information architecture and the information the organization's operations require, as well as the relations between them.

The data balance sheet supports the management's decision-making ability and serves the information-related needs of the organization's customers and stakeholders. The data balance sheet is also an element of information management and the associated risk management and internal control.

Regular evaluation of information security and data protection is part of the organization's information management. The purpose is to ensure the operability and availability of the services offered, the quality of data and the security of the information technology solutions in place. A further goal is also to secure the operation of the information security management and control systems related to the service production.

2.3. The data balance sheet as a tool for internal and external control

An organization must ensure that its internal control has been properly organized. The management is responsible for the appropriate organization and sufficient extent of internal control. It is in the organization's interests to efficiently control its information processing systems and to review them by way of internal and external audits. On the other hand, there is also a strong aspect of general legality control. The data balance sheet satisfies both needs. It also serves the need for information of the authorities responsible for legality control.

A data balance sheet is prepared for one review period at a time. This means the issues described and reviewed in the document can be systematically followed. The review period may be a calendar year or another period determined on the basis of the organization's needs. From the perspective of the organization of internal control and risk management, the data balance sheet may also be integrated with the organization's overall financial statements or annual review process, performance-based management or results reporting.

3. HOW TO PREPARE A DATA BALANCE SHEET

The purpose of the data balance sheet is to describe the current status of data processing and assess the realization of data protection and information security. The data balance sheet also reviews development needs related to data processing and the development measures required.

The data balance sheet may describe, for instance:

- the information resources the organization controls
- the organization's information architecture
- the quality and availability of the data possessed by the organization
- the data processing procedures and principles
- measures taken to protect the information
- measures taken to control the use of information
- the ways in which the rights of data subjects are realized in data processing

The data balance sheet includes an evaluation of any development needs relating to data processing and the necessary development measures.

At least those responsible for information technology, data protection and information security and the organization's core activities may participate in preparing the data balance sheet.

3.1. Information to be included in the data balance sheet

The information included in the data balance sheet may vary, depending on sector in which the organization operates and the nature of its operations. Examples of issues which may be included are given below.

3.2. Information resources controlled by the organization

An organization collects and processes information in a number of information systems and solutions. The management team does not always have a clear understanding of what kind of information the organization possesses. The processing of separate pieces of information in separate information systems is highly resource-intensive and poses a threat for the realization of data protection and information security.

From the perspective of the processing of personal data, it is important to evaluate the various personal data files created for various purposes, their information content and the reasons for maintaining such files. From the perspective of good practice in information management, an organization must have a clear understanding of its information systems, and it must ensure the quality and availability of the information.

When reviewing the information resources, it is appropriate to also review issues such as the level of protection applied to the resources, confidentiality, and the sensitive nature of the information at the same time. Identifying information flows between information resources is important since the management of ever increasing information flows leads to questions such as who is the data owner. A description of the information resources and information flows may be prepared for the data balance sheet, or such descriptions may be separately maintained by the organization, as architecture descriptions or other similar descriptions.

The data balance sheet may include a description of the organization's key information resources and information flows, as well as an assessment of the quality of the information. It may also describe the key indicators relevant to data processing, such as the number of information units processed, items of information received and disclosed, and disclosure transactions. The assessment of data quality is closely related to the assessment of the value and availability of the information.

The quality of information may be assessed from different perspectives, such as:

- the procedures and criteria related to quality assessment
- the results of quality assessment : the
* accuracy
* necessity
* completeness
* currency
of information.

3.3. The procedures and principles applied to data processing

As regards procedures, the description may include aspects such as:
- the most important laws and regulations affecting the processing of information
- the operating principles
- code of practice
- information security and contingency plans
- other guidelines and instructions on data processing
- procedures and agreements related to the outsourcing of data processing
- procedures and agreements related to the maintenance and procurement of information systems

When evaluating the data processing process, the entire life cycle of information should be considered. As regards the operating principles of data processing, issues to be assessed may include the following:
- procedures related to access to and disclosure of information
- administration of user rights
- data protection and information security requirements, particularly as regards electronic data interchange.

The data balance sheet provides an assessment of whether the organization's personnel has the necessary information concerning the existence of the data in the public sphere, its confidentiality, and the procedures applied to data protection, as well as the information security arrangements and the division of responsibilities. The purpose is also to assess the provision of personnel guidance and training and the ways in which the organization ensures instructions and training are kept up to date.

3.4. Data security

The data balance sheet may describe how the controller performs the necessary technical and organizational measures to protect personal data against unauthorized access, accidental or illegal destruction, amendment, disclosure, or transfer, or other illegal handling.

The data balance sheet may include a review of:
- the principles and procedures related to data protection
- the principal objectives and means of implementation related to information security
- the information security management standards applied
- internal and external evaluations
- risk management procedures
- the organization of information security
- responsibilities and the development process, procedures.

3.5. Monitoring and control of data processing

The organization must ensure compliance with the regulations and guidelines on the implementation of good practice in data processing and information management. Compliance must also be monitored. The measures required by good practice in information management are performed in a manner which takes account of the legal protection of all parties.

The control of data processing may be part of the organization's other internal control and risk management activities. The results of control and the action taken should also be reviewed.

The data balance sheet may describe issues such as:
- assessment and management of risks related to data processing
- the measures implemented for controlling the quality of information resources and information flows
- the measures implemented to control the handling process
- the measures implemented to control data processing by the personnel and partners
- the action and development measures taken on the basis of monitoring and control.

In addition to internal control, the decisions of authorities performing external legality control, the decisions of courts of law, and the impact of such decisions on the organization's operations may also be described. The data balance sheet may also include an evaluation of whether the extent of control and monitoring of data processing is sufficient and whether there are any needs for development.

3.6. Realization of the rights of the data subjects

The realization of the rights of data subjects may be assessed on the basis of the numbers of requests for access and rectification referred to in the Personal Data Act, and the responses to such requests. As regards the provision of information to data subjects, the availability of the description of the file and the privacy policy should also be assessed.

4. ASSESSMENT AND THE DEVELOPMENT TARGETS

The data balance sheet serves as a tool for identifying development and measurement needs, as well as related monitoring and reporting, through an analysis of the current status. Development measures may be related to, for instance, the quality of the data itself, or the data handling process. They may also focus on the successful introduction of new technology or more generally, the organization's capability to introduce new tools for knowledge-intensive work.

As regards the central government organization, information on compliance with the requirements concerning the level of information security laid down in the government decree (681/2010) may also be included in the data balance sheet.

Conclusions may be drawn from the data balance sheet. - The operations and data processing have complied with the good practice in data processing and information management. - The monitoring and control of data processing has been successfully carried out in compliance with legislation, regulations, and internal guidelines. - The monitoring and control of data processing has revealed development needs or deviations; the measures taken have been listed separately.
The data balance sheet may include, for instance: - the sub-areas of data processing concerning which development targets have been identified; - the development targets and a review of potential solutions; - a review of the success of the development measures carried out during the previous review period.

Data balance sheet reporting may be targeted at the organization's management, employees, customers, and other stakeholders, or parties responsible for legality control. The data balance sheet may be a dynamic document, the contents of which may be edited according to the target group. For instance, a detailed report on data protection and control may be submitted to the management, while a data balance sheet intended for other stakeholders may contain a summary or an overall review of these issues.

The Personal Data Act and the other acts and decrees referred to in this brochure can be found in the State of Finland legislation database at www.finlex.fi. General information on data protection and the Personal Data Act is available on the website of the Office of the Data Protection Ombudsman at www.tietosuoja.fi. Guidelines issued by the Government Information Security Management Board VAHTI, set up by the Ministry of Finance (www.vm.fi), may also be used when preparing a data balance sheet.

Government organizations may also use the guidelines on the framework for the evaluation of internal control and risk management issued by the Government Controller General of Finland. The data balance sheet may be integrated with the review performed according to these guidelines as an internal control tool (Government Controller General of Finland's guidelines (in Finnish): Valtion viraston ja laitoksen sekä rahaston sisäinen valvonta ja riskienhallinta, VM 23.12.2005, www.wm.fi) The private sector may also use these guidelines as a Finnish source of good risk management practice and its assessment. The guidelines are based on the internationally recognized COSO-ERM framework and the INTOSAI GOV guidelines prepared for the public sector on the basis of the COSO-ERM framework.