CIO Platform Nederland

CAT Data Classification & CEG Information Security

Data Classification Guide

Publication of
CAT Data Classification & CEG Information Security

CIO Platform Nederland, December 2016

CIO Platform Nederland

CAT Data Classification & CEG Information Security

Authors & editorial board

Stoffel Bos (Prorail), Hein Laan (Rabobank), Ronald Verbeek (CIO Platform Nederland)

Reading guide

This document contains a description of good practice for (data) classification. Data corresponds in this context to all data and information, regardless of the medium in which it is stored and regardless of its presentation.

Target audience

This document is especially important for system owners, information managers and (corporate) information security officers.

Acknowledgements

Our thanks go to the Quality Institute Dutch Municipalities (KING) whose Guide to Data Classification served as a source for this document.

Table of contents

1. Introduction

Objective guide

This guide describes good practice for the classification of data. It offers tools to develop, implement and improve a data classification system.

We only talk of classification, but categorisation is also often used within the field. Data in this context corresponds to all data and information, regardless of the medium in which it is stored and regardless of its presentation. Classification in this case corresponds to a process or a system.

All mentioned levels and (retention) periods are a guideline and stem from different sources, including: legislation and PvIB patterns and the guide to Data Classification of Dutch Municipalities.

The classification of data informs the level of measures that need to be taken in order to adequately protect data. It also satisfies the question of whether data falls inside or outside of the baseline.

The importance of classification

The potential damage that may be caused by a threat (e.g. abuse of unauthorised access) to certain data or the possibility that this might occur can be evaluated by a risk analysis. Management needs to indicate which risks are acceptable or which risks should be covered with sufficient measures. The proposed classification method gives a quick indication of the importance of information (systems) and is therefore the basis of a risk analysis.

After classification appropriate measures should be taken to, on the one hand, prevent subsequent violations of safety and on the other hand make sure that no unnecessary effort is required.

2. Classification of data and systems

Data protection is the set standard of taking measures and procedures to protect data.

The aim is: *to guarantee the continuity, integrity and confidentiality of data, but also the provision of data and limiting the impact of any security incidents.*

The protection level of data is expressed in classification levels for availability, integrity and confidentiality of data (processing systems):

- **Availability**: how much and when data is accessible and when it can be used. The distinguishable levels are: *Basic, Low, Middle, High or 0,1,2,3*
- **Integrity:** the conformity of data with reality and confirmation that nothing has been wrongly withheld or has disappeared (accuracy, completeness and timeliness). The distinguishable levels are: *Unknown, Low, Middle, High or 0,1,2,3 (Unknown, Assumed Correct, Verified Correct, Proven Correct).*
- **Confidentiality:** the authority and possibility to mutate, copy, add, destroy or to take note of data by a defined group of users. The distinguishable levels are: *Public, Low, Middle, High or 0,1,2,3*

The levels stated above are based on NORA: (Nederlandse Overheid Referentie Architectuur: Dutch Government Reference Architecture). The baseline is usually A,I,C = L,L,L[1]

By assigning classification levels to data and / or information systems we make the (required) security levels known. On this basis, the security requirements and what measures should be taken will be decided on.

The following factors exert influence on the adequate security measures: policy principles, architectural principles, security requirements (and how to interpret these).

A classification method helps to determine whether the process or system is inside or outside the baseline. If the classification is higher than normal, additional measures are required. Sometimes these measures are part of the application control (within the application). Sometimes they have already been developed in an earlier conducted risk analysis, or a risk assessment is carried out within the organisation by the implementation of a risk analysis with more appropriate measures.

2.1 Risk analysis & residual risks

An organisation that processes data and uses information systems runs a certain risk due to the vulnerability of data and the fact that these systems are vulnerable to threats from inside or outside. Conducting a risk analysis supports management in identifying the risks that are run and how big these risks are. This will help to determine which security measures should be taken in order to reduce risk. Classification is an important tool to determine the severity of a risk and the scope of a measure, especially when translating risks to measures. The proposed classification guide may be regarded as a simplified form of risk analysis.

With a risk analysis threats are identified and mapped. For each threat, the probability of its occurrence is determined; consequently this analysis calculates the damage that might occur if a threat occurs. After the analysis, it is determined how the risk can be mastered, or reduced to an acceptable level: taking data protection measures. In addition to this risk analysis a cost-benefit analysis is performed. Not every risk needs to be covered in advance: if the cost of measures to reduce the risk are greater than the potential harm, the owner of the data can decide to accept the risk.

[1] In international context the order is generally: Confidentiality, Integrity and Availability (CIA). In this publication we use the order of Availability, Integrity and Confidentiality that is used in Dutch security practise.

3. Data classification policy

In this chapter, additional policy frameworks are given as an example that can be used as a separate policy next to the organisation's data protection policy.

Example policy:

The data protection policy of <company name> describes the standards for availability, integrity and confidentiality of data. The various levels of availability are:

- **Basic**: The data can be unavailable for a longer period of time without any consequences. This unavailability has no consequential damage.
- **Low**: The data or service may fail occasionally. The business process allows incidental downtime. The continuity should be resumed within a reasonable period. Unavailability can cause some direct or indirect damage.
- **Middle**: The data or service should almost never fail. The business process allows hardly any downtime. The continuity should be resumed soon. Unavailability can cause serious direct or indirect damage.
- **High**: The data or service only allows downtime in very exceptional circumstances, for instance as a result of a calamity. The critical business process does not allow any downtime. The continuity should be resumed very quickly. Unavailability can inflict (very) extensive damage.

The various levels of integrity are:

- **Unknown**: The data may be altered. No extra protection of integrity is required. Breach of integrity results in no consequential damage.
- **Low**: A business process utilising this data does allow some (integrity) mistakes. Security on a basic level is required. Breach of this classification can cause some direct or indirect damage.
- **Middle**: A business process utilising this data allows few (integrity) mistakes. Protection of integrity is absolutely essential. Breach of this classification can cause serious direct or indirect damage.
- **High**: A business process utilising this data does not allow any (integrity) mistakes. A breach of integrity can cause (very) extensive damage.

The different levels of confidentiality are:

- **Public**: All data is generally accessible to everyone. Breach of this classification is not possible.
- **Low**: Data which may or must be accessible to all employees. Confidentiality is low. Violation of this classification can cause some direct or indirect damage.
- **Middle**: Data which is only accessible to a limited group of users. Data is made available based on trust. Breach of this classification can cause serious direct or indirect damage.
- **High**: This concerns sensitive data which should only be made available to the immediate recipient. Breach of this classification can cause (very) extensive damage.

The labelling of data as a response to the above is usually: Public, Internal, Confidential and Secret.

4. Principles for classification

The following principles are the basis for (data) classification:

1. The owner of the data (often the process owner) determines the required security level (classification). Legal requirements are explicitly stated. The owner of the data determines who gets access to what data.
2. We aim for the 'lowest' possible classification level as every higher classification level leads to unnecessary costs. The government, for example, has to make data available in the context of transparency to as many people as possible.
3. The classification table covers all data sets, data carriers and information systems.
4. Parts of a chain can have different classification levels. Actions are based on the component with the highest classification level in the chain.
5. The object of classification is the data. The classification that is determined by the type of data also applies to the higher levels of the information system (or information services). This means that if the system processes confidential data the whole system is specified as confidential unless measures have been taken for that higher level in the information system. All classifications of all business-critical systems are clearly set by the owners and need to be checked on an annual basis by the CISO (Chief Information Security Officer).

In all cases the owner of the data should be supported by security specialists, such as the (Corporate) Information Security Officer to determine the classifications. The starting point is the Information Security Baseline which should be adopted within an organisation. If more measures are needed these should be adjusted to the risks, taking the technical possibilities and the costs of the required measures into account. This is often situation dependent.

Higher demands are placed on the protection of the data when the data becomes more and more sensitive or if it poses a higher risk within the context in which it is used.

5. Security requirements per classification level

5.1 Availability

As opposed to integrity and confidentiality, availability makes no demands on the content of the data. Therefore, there are no special measures for authentication, authorisation, monitoring and security, unlike integrity and confidentiality. As the availability standards vary per service the classification level of availability should always be specified.

Definition

Availability is defined as "characteristics of the whole IT service, systems, components and data carriers which influence the time a product or service (and hence its data) is available to the authorised user; at the time these should be available". Availability is measured by the Mean Time Between Failures (MTBF). This is the average time between the recovery from one incident and the occurrence of the next incident. The values as listed in the table below are an example. These values must be determined by the organisation itself.

Availability standards

The standards for Office Automation (OA), Intranet of <company name> and the added services are *(please note: this can be completed per system / classification):*

- OA (basic and plus applications): 99,5% availability on working days between 7:30 and 18:00
- Intranet <company name>: 99,5% availability on working days between 7:30 and 18:00.

Required classification		
Working hours	From 08:00 to 17:00 from Monday to Friday except on public holidays.	
Availability during working hours	99,6%	(min.)
Availability outside working hours	96,1%	(min.)
MTBF	100 days	(min.)
MTTR (for failures longer than 3 minutes)	4 hours	(max.)
Number of failures:		
3 minutes or shorter:	4 per month	(max.)
Longer than 3 minutes	1 per month	(max.)

Importance classification		
Working hours	From 07:00 to 21:00 from Monday to Friday except on public holidays.	
Availability during working hours	99,6%	(min.)
Availability outside working hours	96,1%	(min.)

Essential classification		
Working hours	24 hours a day, 7 days a week, except on public holidays.	
Availability	99,9%	(min.)
MTBF	200 days	(min.)
MTTR (for failures longer than 3 minutes)	4 hours	(max.)
Number of failures:		
3 minutes or shorter:	1 per month	(max.)
Longer than 3 minutes	1 every six months	(max.)

5.2 Integrity

The topic integrity can be divided into two parts: the integrity of data communication and the storage on the one hand (i.e. not related to the organisational process itself) and the integrity of data in the applications or practical (i.e. related to the organisational process itself) on the other hand. Integrity is linked to the application and is always situation dependent and depends on the requirements of a specific process. For the functional integrity of the data a minimal set of standards is drawn up for which additional arrangements can be made per service and / or application.

Definition

Integrity indicates the degree to which the data is current and correct. Characteristics include accuracy, completeness and timeliness of transactions.

Security standards

The following table describes the security requirements (and measures) per classification level, subdivided into requirements for authenticity, authorisation, monitoring and security. The retention periods are indicative. These depend on a companies' rules and regulations, but also on legislation such as the Public Records Act (Archiefwet).

Level	Authentication	Authorisation	Monitoring	Security
Unknown	None	None	None	None
Low	Authentication 'basic' is required.	Authorisation is required.	Record authentication (correct and wrong) and the time. Record relevant input and output of an IT-system or service. Store monitoring data for a period of 6 months[2].	Input validation. Check for changes during transport. Transport security or message security Data: the version of the used data is known.[3] [4] After execution of the service changed data remain consistent.
Middle	Authentication 'moderate' is required.	Authorisation is required.	Record authentication (correct and wrong) and the time. Record relevant input and output of an IT-system or service. Store monitoring data for a period of maximum 2 years or longer when suspecting a security incident.	Input validation. Check for changes during transport. Transport security or message security Data: the version of the used data is known. Changes are only made in the source. After execution of the service changed data remain consistent.
High	Authentication 'high' is required. Strong authentication is required.	Authorisation is required. The 4-eye principle is required.	Record authentication (correct and wrong) and the time. Record relevant input and output of an IT-system or service. Store monitoring data for a minimum period of 3 years when suspecting a security incident. Record the initial state of the to be changed data.	Input validation. Check for changes during transport. Message security Data: Data are not stored outside of the source (except for availability) and are not changed outside of the source. After execution of the service changed data remain consistent.

De authentication levels refer to the required security mechanism:

- **Basic**: authentication is based on what is known (name and / or password).

[2] Unless this is not in conflict with laws regarding the recording of data.

[3] It is about the source of the data or a copy of the data and the time of the data used.

[4] Rules relating to the exchange of information with third parties are defined in a supply contract. Also rules regarding integrity and confidentiality are defined here.

- **Moderate**: authentication is based on what is known and on something in possession (for instance: a token, smart card or certificate).
- **High**: authentication is based on a (personal) feature, for instance an iris scan or a finger print scanner.

The authorisation levels refer to the method that performs the check. From level 'protected' (low and middle) authorisation is required. From level 'high' the 4-eye principle is also required. The 4-eye principle consists of one person who documents and one person who approves.

In the column 'Monitoring' at the levels 'protected' and 'high', the term 'relevant' is used. Which data is 'relevant' is at the discretion of the owner. Examples and guidelines for relevant data are master data (data on which other data are based), data in a database and core data, privacy sensitive data and data protected by law and regulations. In case of data transport message security is preferred over transport security. However, transport security might be easier and / or cheaper to implement. Therefore, the decision for transport security and message security is left open for the classification level 'protected'. Message security should be applied to the classifications 'high' and 'absolute'.

5.3 Confidentially

Definition

The authorisation and the possibility to mutate, copy, add, destroy or take note of data by a defined group of users. The different levels are: public, internal, confidential and secret.

Confidential data includes:

- Data that can be traced directly or indirectly to persons (personal data, medical records etc.)
- Company sensitive data (confidential business information, competition sensitive data)

Security measures

The table below describes the security demands (and measures) for each classification level, divided into the requirements for authentication, authorisation, monitoring and security.

Level	Authentication	Authorisation	Monitoring	Security
Public	None	None	None	None
Low / (Internal)	Authentication 'basic' is required. Idle session timeout after 'x'-period of being idle. Idle user session timeout after 120 minutes. Block user after 3 failed consecutive authentication attempts. Authentication 'basic' is required to unblock.	Authorisation is required (member of an organisation).	Record repeated incorrect authentication and time.[5] Store monitoring data for a period of 6 months.	Output validation. Encryption during transport outside the network of company <company name> via transport security or message security. Copies of data should also be protected.
Middle (Confidential)	Authentication 'moderate' is required. Idle session timeout after 'x'-period of being idle. Idle user session timeout after 120 minutes. Block user after 3 failed consecutive authentication attempts. Authentication 'moderate' is required to unblock.	Authorisation on a 'need to know basis'	Record repeated incorrect authentication and time. Store monitoring data for a period of 2 years.	Output validation. Encryption during transport or via intermediate stations inside or outside the network of company <company name> via message security. Copies of data should also be protected. Minimise the number of copies. Message security.
High (Secret)	Authentication 'high' is required. Idle session timeout after 'x'-period of being idle. Idle user session timeout after 120 minutes. Block user after 3 failed consecutive authentication attempts. Authentication 'high' is required to unblock. No SSO are permitted.	Authorisation on a 'need to know basis'	Record repeated incorrect authentication and time. Store monitoring data for a period of 7 years.	Output validation. Encryption during transport or via intermediate stations via message security. Encrypted storage of data. Minimise transport of data. Transport and storage only within the fixed network of <company name>. No copies allowed except for availability.

The authentication levels refer to the required security mechanism (see previous paragraph). Competition sensitive data refers to the organisation, which entails: the organisation <company name>, an organisational unit or a service.

[5] 'Record repeated incorrect' means in the context of monitoring if an identity consecutively three times incorrectly authenticates. After the successful login, the counter "put to zero".

6. Determining the classification levels

The previous chapters described the required context when assigning classification levels: the policy principles, the architectural principles and the security requirements. This knowledge facilitates the classification of data. This chapter discusses how to proceed step by step.

Step 1: Legal requirements

The first step of data classification is to investigate which laws and regulations impose requirements on the use, distribution or storage of the data.

The Dutch **Data Protection Act (DPA)** especially sets high standards on the processing of personal data in which the concept 'appropriate security measures' plays a role. In order to consider carefully what is and what is not permitted, it is advisable to consult with a lawyer or a legal service.

We use the term data breach when there is a failure to protect personal data (as referred to in article 13 of the Data Protection Act). In case of a data breach personal data are exposed to loss or unlawful processing – i.e. this is the kind of exposure for which security measures should provide protection.

In May 2018 the new European General Data Protection Regulation becomes effective. The consequences are currently (2016) not completely clear, but the effects will be similar to the changes made in the Data Protection Act.

Step 2: Responsibilities concerning data

For assigning classification levels it is important to record who has responsibility concerning data and / or information systems:

1. Determine who can use what data, who is authorised to determine the security level (taking into account the limitations by law) and what interest the 'business' has for using the data.
2. Also, determine who uses the data and / or the information systems and which authorisations they have. This is relevant to determine the risks. Data that is available to only a few is less vulnerable than data that is distributed widely.

Although the data owner is responsible for classification, knowledge about use, distribution and storage and knowledge about the security context lies with other parties concerned. When classifying data, the owner of the data can request help from the responsible functional manager and the person with the role of Company Information Security Officer (CISO).

Step 3: Analysis of critical business processes

Classification levels are derived from the results of the data and the importance of the business process in which these data take part. Furthermore it is of importance to determine the interests of the organisation's business processes and how these processes are supported by IT facilities.

The analysis is performed using the model questionnaires in appendix 2. These questionnaires directly show the required classification level for availability, integrity and / or confidentiality for the data asset.

Filing completed questionnaires in the context of reproduction is strongly recommended in order to provide for, for instance, an audit which requests background data, but also to make comparisons in case of future reclassification.

The results of this step can be displayed in a compact summary for the particular business processes, like in a table below.

Process	Availability	Integrity	Confidentiality
Process "x"	Moderate	High	Confidential
Process "y'	High	High	Secret
Process "z"	High	High	Public

Step 4: Findings: criteria for determining a good baseline

Classification is not an exact science. Determining the classification level is the result of a risk assessment in which the 'value' of data is determined. Since a 'value' is not always measurable, awarding a classification level is sometimes arbitrary. In those cases, a decision should be made between the value and the risk of data loss. The classification level and the corresponding security measures and requirements should always 'suit' the data to be protected.

Article 13 of the Dutch DPA identifies 3 criteria that need to be used when deciding on the technical and organisational measures:

1. The state of the art technologies
   - One should first determine what technical measures are available at that time;
   - With regard to the available facilities outdated techniques are no longer classified as appropriate;
   - This entails that the person responsible for deciding which technical measures will be used should find a balance between the technical facilities that are used for processing and the facilities that are used for the protection of personal data;
   - The person responsible should repeat this analysis periodically.
2. The cost of implementation
   - The person responsible should decide between the available technical and organisational measures: in all fairness one should determine the proportionality between the cost of security and its impact on the protection of personal data;
3. The risk that processing brings
   - This defines the risk those involved or the person responsible run in case of loss or unlawful processing of personal data: the more the risk increases the more the measures should be increased proportionally.

The classifications can be best implemented in a workshop setting. This has a learning effect, gives commitment, leads to cooperation and above all leads to a weighted average.

Step 5: The result

The results of this analysis translate into a classification report with the completed questionnaires as appendices.

Appendix 1: Classification guide

The classification process at <company name> is supported by three questionnaires, which help to determine the impact on business processes:

a) Questions about availability
b) Questions about integrity
c) Questions about confidentiality

The impact on the business is rated on a 5-point scale.

Scale:

1. Negligible
2. Slight damage
3. Moderate damage
4. Major damage
5. Threatens the existence of the organisation

From the results of the business process reviews (the 5-point scale) a translation can be made to a 3-point scale that is used for the Modelling of BIA.

The classification used for integrity and confidentiality is represented as follows:

Business impact	**I-classification**	**V-classification**
1	0 – Unknown	0 – Public
2	1 – Low	1 – Low / Internal
3 + 4	2 – Middle	2 – Middle / Confidential
5	3 – High	3 – High / Secret

Appendix 2: Classification questionnaires

This appendix can be used as a separate document and serves as a basis to determine the various classifications. Fill in the data below.

Document owner	
Function	
Organisational unit	
Phone number	
Enter final date	

The result of the investigation concerning the CIA triad for the process <process name> of <company name> indicates a classification of the following levels:

a) Confidentiality :
b) Integrity :
c) Availability :

Conclusion:

The process <process name> falls within / outside the baseline data protection and requires / does not require extra additional measures. These measures may already exist as part of a fixed plan or a comprehensive risk analysis is required.

Is there cause to deviate from the drawn conclusion (by the system owner)?

If there is a deviation: is the residual risk acceptable? YES/NO[6]

Thus signed at (business/place):

on (date):

Signature:

Name of Owner:

[6] Delete where appropriate.

A – Questionnaire availability

In the context of availability, it is important to consider at the magnitude of damage resulting from a certain downtime period.

a) Which group of users is effected by a downtime of the data asset? How large is this particular group? What is on average the estimated number of simultaneous users of the data asset?
b) What should be the opening hours for the data asset? What availability percentage is desired?
c) Which frequency of system failure is considered acceptable? (per month / per quarter / yearly)
d) Is there a business continuity plan as data asset?
e) Are there critical downtime moments (for instance payroll at the end of the month, special reports, elections, opening hours and calamities)?
f) Acceptable maximum downtime?

Business impact scale:

1. Negligible
2. Slight damage
3. Moderate damage
4. Major damage
5. Threatens the existence of the organisation

Business consequence	**Business impact**				
When maximum damage	**Hour**	**Day**	**Week**	**2–3 weeks**	**month**
Management decisions How detrimental is it if due to unavailability the wrong management decisions are taken?					
Direct loss of revenue Will it result in loss of revenue if the business information is not available?					
Public trust Will trust be harmed or will it result in a damage of image if the data asset is not available?					
Extra costs Should extra costs be incurred if the data asset is not available?					
Accountability Can the unavailability of an application lead to any kind of accountability?					
Recovery What will it cost to tackle a backlog of work after the restart?					
Employee morale Will it have any negative impact on the morale of users if the application is not available?					
Fraud If the data asset is not available can this lead to fraudulent acts?					
Total score In summary: what is the most severe damage which can occur in case of an outage at the most critical moment?					

B – Questionnaire Integrity

When categorising integrity, it is important to determine which implications could be the result of errors in the data. This applies both to intentional errors (or fraud) or unintentional errors. Confidentiality involves the question of whether someone else is allowed to see the data, integrity questions whether someone else is allowed to modify the data. Core concepts are accuracy and completeness.

a) Are the data in the data asset the basis for management decisions?
b) Which retention period applies? (records act, Data Protection Act, tax laws)
c) Will there be a systematic check for accuracy or completeness?
d) For what kind of workplaces should data be made available (any time and everywhere, at home, in classrooms or work stations)?
e) Can a user obtain an unfair advantage by changing data intentionally (commit fraud)?
f) What is the maximum allowable data loss after an outage?

Business impact scale:

1. Negligible
2. Slight damage
3. Moderate damage
4. Major damage
5. Threatens the existence of the organisation

Business consequence	**Business impact**				
When maximum damage	**Hour**	**Day**	**Week**	**2–3 weeks**	**month**
Management decisions How detrimental is it if due to unavailability the wrong management decisions are taken?					
Direct loss of revenue Will it result in loss of revenue if the business information has been altered due to unauthorised changes?					
Public trust Will it result in a damage of image if incorrect data is used?					
Accountability Can the incorrectness of data lead to any kind of accountability?					
Employee morale Will it have any negative impact on the morale of users if they have to work with incorrect data?					
Fraud What is the impact of any act of fraud?					
Total score In summary: given the above scores (and any other possible consequences) what is the most severe damage which can occur because of errors or unauthorised changes? (this should on average be minimally equal to the most severe damage on an individual basis).					

C – Questonnaire Confidentially

To determine whether and how confidential data is, it is important to know the business impact in case of unplanned or unauthorised disclosure or data being publicly disclosed. A special category of confidential data are personal data. Personal data must be managed in compliance with the Data Protection Act. This act allows flexibility but sets conditions for data processing, in particular the diligence with which personal data is handled.

a) Are data stored or processed in the data asset traceable to private individuals?
b) Does the system contain any special personal data as referred to in the Data Protection Act, article 16?
c) Are data from the data asset combined with data from other systems traceable to private individuals?
d) Does the data asset contain any competition sensitive data (for instance the structure of rates, contracts)?
e) Does the data asset contain data under embargo?
f) Does the data asset contain data that should only be available to a particular target audience? (for instance licence restrictions).
g) Does the data asset contain data which can be used to commit fraud? (for instance identity fraud, credit card numbers, password files).

Business impact scale:

1. Negligible
2. Slight damage
3. Moderate damage
4. Major damage
5. Threatens the existence of the organisation

Business consequence	**Business impact**				
When maximum damage	**Hour**	**Day**	**Week**	**2-3 w**	**Month**
Management decisions How detrimental is it if due to unavailability the wrong management decisions are taken?					
Direct loss of revenue If business information falls into the wrong hands will it result in loss of revenue?					
Public trust How much damage will be done to the company's image if this data is publicly disclosed? How big a negative impact will this have on the trust that customers have in us?					
Legislation Does the system comprise personal data in the sense of the Data Protection Act, article 16?					
Accountability Will disclosure lead to accountability based on legal and contractual obligations?					
Employee morale Will it have any negative impact on the morale or the motivation of users in case of disclosure?					
Fraud What is the impact of any act of fraud resulting from the disclosure of the data?					
Total score In summary: given the above scores (and any other possible consequences) what is the most severe damage that can occur due to unintentional or unauthorised access to this data? (this should on average be minimally equal to the most severe damage on an individual basis).					

Appendix 3: Rating scale

Organisations should determine for themselves whether the damage levels listed below are appropriate to them or should be adapted if necessary.

	Personal data	**Legal and regulatory obligations**	**Financial loss**	**Policies and the functioning of the organisation**	**Loss of goodwill**
Some damage Business impact = 1 or 2	Discomfort to a person, but does not infringe any law or regulation.	Civil procedure or criminal prosecution resulting in a compensation or penalty less than € 5,000.	Results in direct or indirect losses of less than € 10,000.	Contributes to a part of the organisation not operating sufficiently.	Has a negative impact on relations with other parts of the organisation or the public.
Serious damage Business impact = 3 or 4	A breach of laws or regulations resulting in a slight discomfort to a person or group of persons.	Civil procedure or criminal prosecution resulting in a compensation or penalty between € 5,000 and € 50,000.	Results in direct or indirect losses between € 10,000 and € 100,000.	Disadvantages a well operated and / or functioning part of an organisation.	Has a negative impact on relations with other organisations or the public; resulting in negative local publicity.
Major extensive damage Business impact = 5	A breach of laws or regulations resulting in a considerable discomfort to a person or group of persons.	Civil procedure or criminal prosecution resulting in a compensation or penalty above € 50,000 or imprisonment.	Results in direct or indirect losses above € 100,000.	Disadvantages a well operated part and / or the entire organisation.	Has a significant impact on relations with other organisations or the public; resulting in widespread negative publicity.