TLP:CLEAR

CONCLUSION

DATA CLASSIFICATION DIRECTIVE

Author
Roel Gloudemans
(roel.gloudemans@conclusion.nl)

With the cooperation of
Chris Gralike, Ricky Hoots, Artien Bel, Dennis Pieterse, Paul Schoorl, Curtis Waterval

Status:	Final
Version:	2.1
Best before:	2026-07-08

Version table			
Date	Version	Through	Adaptation
21-09-13	0.1	R. Gloudemans	First draft
22-02-04	1.0	R. Gloudemans	Final version
23-02-22	1.1	R. Gloudemans	Document checked; No changes
24-05-10	1.2	R. Gloudemans	Treating personal data in bulk as special personal data.
24-05-23	1.3	R. Gloudemans	Update with CEO fraud message
24-11-25	1.4	E. Aksoy	English Translation
25-05-10	1.5	J. van Andel	Kleine tekstuele aanpassingen
25-05-19	1.6	R. Gloudemans	Spell/Grammar corrections, reference to Benelux policy instead of ecosystem policy. Backported a change from the Dutch 1.4 version.
25-07-08	2.0	R. Gloudemans	Renaming of confidentiality labels to Traffic Light Protocol scheme
25-07-09	2.1	C.Waterval	Reviewed and added AI-specific classification rules for ISO42001 compliance.

Approval	
Document	Version
Version	1.0
All major versions of this document are approved by at least 5 security officers from different Conclusion companies. Minor changes, such as spelling errors and changes and/or additions to the explanatory notes, are the responsibility of Conclusion's Director Information Security	
*This document is classified as **TLP:CLEAR** information and can be made available (in pdf form) to anyone for whom this policy document is relevant.*	

Contents

1. Summary for the employee

All information within Conclusion must be classified. This is the only way to ensure that the right controls are implemented and that the controls are not unnecessarily burdensome.

Documents are classified based on confidentiality only. The following classifications are used:

Confidentiality & Document Classification		
Label	**Dissemination**	**Example**
TLP:CLEAR (Public)	Can be seen by everyone	• Website • Security policy
TLP:GREEN (Company information)	May only be seen by Conclusion employees and one or more customers	• Conclusion service catalogue
TLP:AMBER (Internal)	May only be seen by a limited group of Conclusion employees and a limited group of employees of a customer. Customers must treat the information as TLP:AMBER+STRICT and may not disclose the information to anyone else.	• Offer • List of security measures taken • Personal data
TLP:RED (Confidential)	May only be seen by a few Conclusion employees and a few employees of a customer.	• Shareholder information • Financial data • Audit reports • Special categories of personal data

These classifications can be set in Office and Mail, after which the corresponding controls are set automatically.

If you are responsible for a larger (structured) dataset or a business process, the information you process must also be classified in terms of Integrity (correctness & completeness) and availability. The relevant labels for this can be found on page 8.

The controls that must be implemented because of the classification can be found in the other directives documents that are a tool for the owners of infrastructure, applications and processes to help them managing the risks.

For information that is TLP:AMBER or TLP:RED, non-Conclusion means of communication may not be used. Use of SMS, Whatsapp, Signal, etc. is not allowed. Requests of a confidential nature through these channels must be ignored, even if they appear to be genuine.

If in doubt, contact your supervisor. If the communication states that your supervisor must be left out of the loop, then the message is definitely fake.

2. Introduction

2.1 Location

This policy document and all other documents referred to in this document can be found on the "Security"[1] page of Start Your Day.

2.2 Background

Conclusion recognizes that not all information has the same importance regarding availability, integrity, and confidentiality

Information classification is a method of determining how valuable information is to the business processes and the stakeholders in these processes. Based on the classification, the standard set of controls that should be sufficient for the protection of interests is determined.

Definitions

Availability (continuity, response time).
The extent to which the information must be available within the organization at the time a user needs this information.

Integrity (accuracy, completeness, timeliness, lawfulness).
The extent to which the information within the information systems is complete and accurate. Completeness should also be understood to mean that no more than the necessary information is included in the system.

Confidentiality (exclusivity).
The extent to which access to and acquaintance with the information is limited to a defined group of users, who have explicitly declared that they will handle the information systems and the information contained therein in a correct and careful manner.

2.3 Scope

This document describes the data classification, as it is used when information is exchanged between the Conclusion companies and as it is communicated to outside parties.

2.4 Objective

This document specifies what the classification categories are, when information falls into a particular category, how the classification works, and what the responsibilities are.

2.5 Target audience

This document is intended for all employees, with those responsible for large information sets in particular.

[1] https://conclusionfutureit.sharepoint.com/sites/StartYourDay/SitePages/Privacy-&-Security.aspx

3. Classification

3.1 What is Information Classification

The purpose of information classification is to indicate the importance of this information, so that those responsible for information, process, application and infrastructure can take measures to adequately protect the information. These measures must demonstrably ensure that Conclusion does not take unacceptable risks.

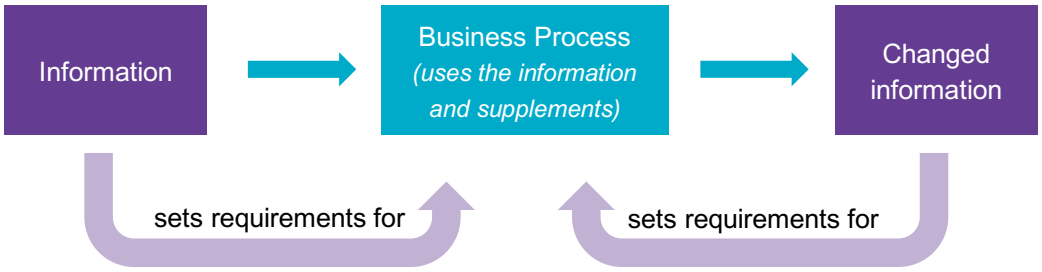


Figure 1, A business process that processes information.

A business process needs information to work and produces new information. Both the classification of imports and exports set requirements for the controls and technology used in the process.

The information classification establishes the link between the importance of the information and the minimum controls that are desirable to safeguard Conclusions' interest.

If a certain control is not implemented, it is noted as a vulnerability in the process. Subsequently, a risk analysis examines whether it is necessary to implement the control in the context of the process, or whether the absence does not lead to unacceptable risks.

The recommendation is to implement controls as close to the information as possible. By encrypting a confidential Word file, it can, for example, be stored in Teams and sent by e-mail. Otherwise, a special environment would have to be set up for this.

3.2 Conclusion classification scheme

3.2.1 Classification table

Conclusion uses a three-by-four matrix for the classification. In the table each classification for each category has a specific denomination. A level can also be used to refer to the classification. The level is indicated by a number.
For confidentiality Conclusion uses the internationally accepted Traffic Light Protocol (TLP)

All data classification levels of Conclusion			
Level	Availability	Integrity	Confidentiality
1	Very low	Not checked	TLP:CLEAR (Public)
2	Low	Correct	TLP:GREEN (Company information)
3	Middle	Important	TLP:AMBER (Internal)
4	High	Essential	TLP:RED (Confidential)

Rules regarding data classification						
#	Control	1	2	3	4	
R-DC-0	**Classification of datasources must be reviewed annually** This typically happens during the annual risk analysis. Classification must be re-evaluated after Incidents with unexpected impact.	✓	✓	✓	✓	

3.2.2 For documents

Documents within Conclusion are only classified for confidentiality. Integrity and availability do have significance, but only for the place where the documents are stored and the process of modifying the information.

Confidentiality & Document Classification		
Label	**Dissemination**	**Example**
TLP:CLEAR (Public)	May be seen by everyone	• Website • Security policy
TLP:GREEN (Company information)	May only be seen by Conclusion employees and specific customers	• Conclusion service catalogue
TLP:AMBER (Internal)	May only be seen by a limited group of Conclusion employees and a limited group of employees of a specific customer. The customer must treat this information as TLP:AMBER+STRICT and may not disclose it to other parties.	• Offer • List of implemented security controls • Personal data
TLP:RED (Confidential)	May only be seen by a few Conclusion employees and a few employees of a specific customer.	• Shareholder information • Financial data • Audit reports • Special personal data and personal data in bulk (100+ people)

Rules for handling documents					
#	Control	TLP:CLEAR	TLP:GREEN	TLP:AMBER	TLP:RED
R-DC-1	Documents are always classified	✓	✓	✓	✓
R-DC-2	The document always indicates whether it contains personal data			✓	✓
R-DC-3	The creator classifies a document	✓	✓	✓	✓
R-DC-4	Further distribution of the document must be reported to the owner.			✓	
R-DC-5	The recipient may not distribute a document further.				✓
R-DC-6	Deviations/changes to the classification must be reported to the owner.			✓	
R-DC-7	The recipient must not change the classification.				✓
R-DC-8	In the case of personal data, the retention period must be stated on the document[2].			✓	✓

3.2.3 For (structured) data sources

For information in databases and other types of data storage, the classifications for integrity and availability apply in addition to the confidentiality classification. If these classifications are important for a document, the business process must ensure that the document is stored in a source of information that has taken the appropriate measures in terms of integrity and availability. Based on the integrity classification the document may, or may not be processed using Artificial Intelligence.

The measures associated with each classification can be found in the various directives' documents.

[2] See "Retention Periods Guideline" for help in determining the retention period

Integrity

Classification for integrity		
Label	**Description**	**Example**
Not checked	Uncontrolled modification of the information has no negative effects.	• Internal Newsletter
Correct	It must be possible to state with some certainty that the information is correct and complete. Incorrect or incomplete information leads to confusion.	• Payslip • Audit report • Website
Important	It is important that the information is correct. Incorrect information leads to damage to Conclusion or a single customer or data subject.	• Offer • Personal data
Essential	Incorrect or incomplete information will result in irreversible damage for Conclusion and/or one or more customers or data subjects.	• Special categories of personal data • Large financial transactions

The integrity classification also has a direct relation with the use of artificial intelligence. The AI Act of the European Union declares 4 different risk categories which translate directly to the integrity scale use by Conclusion

Classification for integrity and AI risk categories	
Label	**Risk category**
Not checked	Minimal risk, This category includes, for example, AI systems used for video games or spam filters. Most AI applications are expected to fall into this category.
Correct	Limited risk, AI systems in this category have transparency obligations, ensuring users are informed that they are interacting with an AI system and allowing them to make informed choices.
Important	High Risk, AI applications that are expected to pose significant threats to health, safety, or the fundamental rights of persons.
Essential	Unacceptable, AI applications in this category are banned

As a result of this legislation several rules apply to AI. These are part of the directives for people and process and SDLC and projects. As special personal data falls within the “Essential” classification for integrity with related risk category “Unacceptable” AI applications using this data are prohibited.

Availability

Availability Rating		
Label	**Description**	**Example**
Very low	It's okay if the information isn't available.	• Pictures of the last team outing
Low	Information that is supposed to be available, but where the activities can wait.	• Start Your Day
Middle	Information that is supposed to be available, but where the activities cannot wait long.	• Website • Accounting • Teams
High	Information to support vital customer processes or Conclusion.	• Traffic data from the Dutch Railways.

3.2.4 Classification and commonly used systems

Suitability of commonly used storage media			
Supply	Confidentiality	Integrity	Availability
Teams	TLP:GREEN	Correct	Middle
Teams with encrypted files	TLP:RED	Important	Middle
email	TLP:GREEN	Not checked	Low
e-Mail Encrypted	TLP:RED	Important	Low
USB-stick	TLP:GREEN	Not checked	Very low
Laptop	TLP:GREEN	Correct	Low

Implement automatic labelling of information whenever possible.

Especially for information that is classified as middle and high, non-standard means of communication must never be used. Use of SMS, Whatsapp, Signal, etc. is <u>not</u> allowed. Requests of a confidential nature through these channels must be ignored, even if they appear to be genuine.

If in doubt, contact your supervisor. If the communication states that contacting your supervisor is not allowed, then the message is fake.

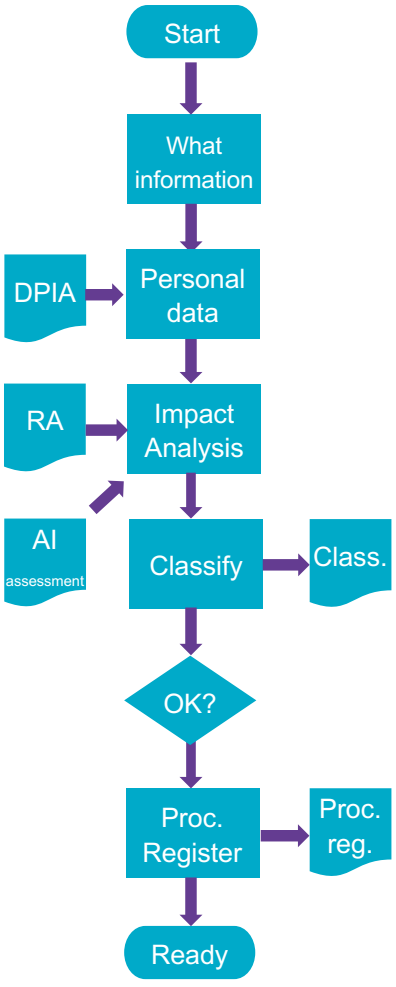
4. Classification Process

Classification of information is an important tool for determining the appropriate controls to protect the information. In practice, too many controls is just as bad as not enough. This results in complex operations, annoyance and costs.

Several players are involved in the classification of information. The most important of these is the person responsible for the information, a role often referred to as the "owner". The owner is responsible for a correct classification and must ensure that the information is properly protected. The owner is assisted by the security and privacy officers.

Documents are classified by the owner (creator) or are given a classification based on the business process in which they are generated, for example a payslip.

The owner of the information must ensure that those responsible for processes and systems implement appropriate controls to protect the information. Controls that are not implemented must be noted as vulnerabilities and must be included as vulnerabilities in the risk analysis by the owners of the business processes involved.



Owner	Privacy Officer	Security Officer	Definition
R			What information does the classification cover?
R	C/I		Does it contain any personal data? In what quantity? Use the DPIA as input.
R		C/I	Do an impact analysis. Use the risk analysis of the processes involved as input.
R	I	I	Classify the information.
C/I	I	R	Check that the analysis has been carried out in a qualitatively good way.
	R		If necessary, the privacy officer will update the data processing register.

5. Classification and trust

Information is processed at a location. This location is physical and/or digital.
A characteristic of a location is whether it is trusted or not. There are three possibilities:

1. A trusted location, which includes Conclusion's trusted applications and infrastructure (see the "Security Policy Benelux" document for the definition of trust.
2. A controlled location, which is not trusted but in which there are safety measures in place. This includes applications and infrastructure that Conclusion can influence, but which are not trusted. Another example is, for example, a party with which Conclusion has concluded a processing agreement.
3. An untrusted location, these are the applications and infrastructure that Conclusion does not want to and/or cannot exert influence on and that are not trusted. In the physical domain, for example, these are public locations.

If information with a certain classification must be processed from an unsuitable location, additional controls must be implemented. For instance: Screen filters that prevent shoulder surfing.

Trust also plays a role in the context of AI. The AI is either trusted, or it is not. An AI that is not trusted may not be used with TLP:AMBER and TLP:RED data. Either attributes need to be removed to declassify the data to a lower level, or steps like supplier and AI assessment or running it on premise, must be taken so the AI may be trusted.

AI may also be used to generate new data. Generally, the integrity of the input data must at least be at the same level as the output data. Usecases exists where an AI could generate higher quality data from multiple low-quality sources. These cases are allowed, but only after an explicit risk assessment. Data with Integrity classification “Essential” can never be generated by an AI.

		Location type where the information may be processed	Trusted AI	Untrusted AI
Integrity	Not checked	Not trusted		
	Correct	Controlled		
	Important	Trusted		
	Essential	Trusted		
Confidentiality	TLP:CLEAR	Not trusted	Yes, inference & training	Yes, inference & training
	TLP:GREEN	Controlled	Yes, inference & training	Yes, inference
	TLP:AMBER	Controlled	Yes, inference only	No
	TLP:RED	Trusted	Yes, inference only	No

CONCLUSION

CONTACT
security@conclusion.nl