Brand Compliance

GDPR Certification Standard and Criteria

BC 5701:2024

Core criteria

This is a free, condensed version for information purposes.
An official full version can be purchased from
www.brandcompliance.com

A European Data Protection Seal

applicable by controllers and processors in the EEA

Colophon

Publisher

Brand Compliance B.V.
Hambakenwetering 8D2
5231 DC ‘s Hertogenbosch
The Netherlands
www.brandcompliance.com

Authors

Joost Holstvoogd
Piims academy B.V.
www.piimsacademy.com

Christian Oudenbroek
Brand Compliance B.V.

Version

This is a free condensed version for information purposes. This version is *not* suitable for application or certification purposes.

Version approval

The official version of the GDPR Certification Standard and Criteria BC 5701:2024 was approved by the European Data Protection Board (EDPB) on 2 December 2024 as a European Data Protection Seal, in accordance with Article 42(5) of the GDPR.

GDPR Certification Standard and Criteria
BC 5701:2024

A European Data Protection Seal

Criteria for demonstrating appropriate elaboration on and consistent application of the General Data Protection Regulation when processing personal data.

The certification mechanism BC 5701 is a joint development of
Brand Compliance B.V. and

piims academy

The official training institute for the BC 5701

www.piimsacademy.com

Table of contents

Introduction

This GDPR Certification Standard and Criteria BC 5701:2024 (hereafter: the BC 5701) has been developed to help organisations implement Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the 'General Data Protection Regulation' or 'GDPR' for short) in an appropriate manner and to enable them to proactively demonstrate adequate protection of personal data.

The BC 5701 is a European Data Protection Seal as referred to in the second sentence of Article 42(5) of the GDPR.

The BC 5701 can be applied to the processing of personal data in the context of the activities of an establishment of a controller or processor[1] established in the EEA, regardless of the type and size of the organisation and regardless of the nature of the products or services it provides.

The BC 5701 *cannot* be used to certify the processing of personal data by an organisation located outside the EEA, as referred to in Article 3(2) GDPR.

The BC 5701 *cannot* be used to certify personal data processing operations where two or more controllers jointly determine the purposes and means, as referred to in Article 26(1) GDPR.

The BC 5701 is *not* a transfer tool under Article 42(2) GDPR and Article 46(2)(f) GDPR.

Due to the informative purpose of this document, the further content of this chapter has been omitted.

[1] Processing activities carried out (in part) as sub-processing will be certified in the organisational capacity of processor.

1. Subject

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, which entered into force on 25 May 2018, provides a framework for the protection of natural persons with regard to the processing of personal data and the free movement of such data.

Article 5(2) of the GDPR states that the controller is responsible for complying with the principles of the GDPR and must be able to demonstrate compliance, also known as 'accountability'.

Article 24(1) of the GDPR states that the controller shall implement appropriate technical and organisational measures to demonstrate that the processing is carried out in accordance with the GDPR.

Article 42(1) of the GDPR calls for data protection certification mechanisms to demonstrate, as referred to in Article 24(3) GDPR, that controllers and processors comply with the GDPR when carrying out processing operations.

Article 42(5) of the GDPR allows for the development of a common certification, the European Data Protection Seal.

The BC 5701 has been developed according to Article 42 GDPR. It aims to provide a framework for the appropriate elaboration of the GDPR, contribute to the consistent application of the GDPR, and enable organisations to proactively demonstrate the adequate protection of personal data.

2. Normative references

Due to the informative purpose of this document, the content of this chapter has been omitted.

3. Definitions

3.1 Terminology

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

3.2 Abbreviations

C Controller

Used to indicate that the section, objective or implementation requirement applies to an organisation acting as a controller in relation to the target of evaluation.

DPIA Data Protection Impact Assessment

DPO Data Protection Officer

EDPB European Data Protection Board

EEA European Economic Area (EU + Norway, Iceland and Lichtenstein)

EU European Union

Where EU or Member State is used, it must be read as EEA or Member State of the EEA.

GDPR General Data Protection Regulation.

P Processor

Used to indicate that the section, objective or implementation requirement applies to an organisation acting as a (sub)processor in relation to the target of evaluation.

ToE Target of Evaluation

3.3 Symbols

| Delimiter that shall be read as 'and'.

/ Delimiter that shall be read as 'or'.

4. Context of the data processing

4.1 Context of the data processing to be certified C | P

The organisation shall document the context in which it intends to apply the BC 5701. The organisation shall consider internal and external aspects that affect its ability to comply with the GDPR, the BC 5701 and the objectives of the organisation.

Objective **The organisation shall be able to provide all relevant parties, including the supervisory authorities concerned and the certification body, with clearly documented insight into the context of the data processing operations.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

4.2 Scope C | P

The organisation shall determine the Target of Evaluation and the scope for the application of the BC 5701, taking into account:

a. the internal and external aspects identified in Section 4.1;
b. the legal requirements identified in Section 4.3;
c. the other requirements identified in Section 4.4;
d. areas of overlap and dependencies between the Target of Evaluation and the context of the processing operations in terms of activities, parties and systems.

The Target of Evaluation must be meaningful with respect to the message or claim made on/by the certification and should not mislead the user, customer or consumer or data subject.

Objective **The application of the BC 5701 shall be clearly delineated and the delineation shall be meaningfully aligned with the perception of the target group of the processing operations.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

4.3 EU and Member State law C | P

The organisation shall comply with all EU, national and sectoral laws and regulations applicable to the ToE, and insofar it defines the GDPR, taking into account the laws and regulations of all Member States in which the data subjects, targeted by the processing activities, reside.

Objective **The organisation shall have a complete, accurate, up-to-date and consistent understanding of, and shall comply with, the applicable laws and regulations governing the processing of personal data within ToE.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

4.4 Other requirements C | P

Taking into account the internal and external aspects identified in Section 4.1, the organisation shall identify:

- the parties relevant to these aspects;
- the requirements of those parties relevant to these aspects;
- where applicable, the codes of conduct and standards applicable to the organisation and relevant to these aspects.

Objective **The organisation shall have a full understanding of the requirements of relevant laws, codes of conducts and parties for the processing and protection of personal data and their relevance to the target of evaluation.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

5. Organising the data protection

5.1 Commitment of the management C | P

Management shall demonstrate that it is fully committed to achieve the objectives and implementing the requirements of the BC 5701 by:

a. communicating the importance of achieving the objectives and requirements of the BC 5701 and the GDPR;

b. ensuring that policies and data protection objectives are established in relation to the GDPR and the BC 5701;

c. ensuring that the resources necessary to implement the BC 5701 are made available;

d. providing guidance and support to individuals contributing to the implementation of the GDPR and the BC 5701;

Objective **Management shall provide resources, guidance and support for the processing and protection of personal data in accordance with relevant laws and regulations, external party requirements, the BC 5701 and internal business requirements.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

5.2 Policies

5.2.1 Establishing policies C | P

Management shall establish, document and implement data protection policies that:

a. are appropriate to the organisation's processing operations;

b. provide frameworks for setting objectives;

c. include a commitment to comply with the GDPR, the established requirements and the BC 5701;

d. ensure compliance with the principles of data protection by design and data protection by default.

Objective **The organisation shall provide an appropriate and clear framework for adequate processing and protection of personal data, taking into account the organisation's particular facts and circumstances, the processing activities, and the requirements and characteristics of the relevant parties.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

5.2.2 Communicating and implementing policies C | P

Policies regarding data protection shall be:

a. communicated, understood and applied within the organisation;

b. readily available to the relevant staff.

Objective 1 **The internal and external staff involved in the processing shall be familiar with, understand and apply the relevant parts of the policies in the context of their work.**

Objective 2 **The internal and external staff involved in the processing shall be able to easily access the parts of the policies that are relevant to them at any time.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

5.3 Roles, responsibilities and authority

5.3.1 General C | P

Management shall ensure that the roles, responsibilities and authority for the processing and protection of personal data are assigned, communicated and understood within the organisation.

Objective **In relation to the ToE, the organisation shall be structured in such a way that it can continually meet the requirements of the GDPR, of the BC 5701 and of the requirements established in Section 4.3 and Section 4.4.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

5.3.2 Data Protection Officer (DPO) C | P

The organisation shall designate a DPO where:

a. the organisation is a public authority or body, except for courts acting in their judicial capacity;

b. the core activities of the organisation consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

c. the core activities of the organisation consist of processing on a large scale, special categories of data pursuant to Article 9 of the GDPR and personal data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or

d. the designation of a DPO is mandatory by Member State law.

A group of undertakings may appoint a single DPO provided that the DPO is easily accessible from each establishment.

5.3.2.1 Appointing the DPO C | P

The organisation shall determine and document whether the appointment of a DPO is required (see: 5.3.2, a. to d.) and, if so, appoint a DPO.

Objective **The organisation shall correctly determine whether it is required to appoint a DPO, verifiably decide on the appointment of a DPO and, if so, establish the position and appoint a DPO.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

5.3.2.2 Position of the DPO C | P

The Board shall ensure that the DPO:

a. is involved, properly and in a timely manner, in all issues relating to the processing and protection of personal data;

b. is able to perform his or her tasks independently;

c. has sufficient resources to perform his or her tasks adequately;

d. is supported in the performance of his or her tasks;

e. has access to personal data and processing operations;

f. has the necessary resources to keep his or her knowledge up to date;

g. can be contacted by the data subjects on any matter relating to the processing of their personal data and the exercise of their rights;

h. will not be involved in activities that may lead to conflicts of interest.

Objective **The organisation shall support the DPO in the adequate execution of his or her legal tasks.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

5.3.2.3 Tasks of the DPO C | P

The DPO shall, with due regard to the risks associated with processing operations and taking into account the nature, scope, context and purposes of the processing, at least:

a. inform and advise the organisation and its employees of their obligations pursuant to the GDPR, other EU and Member State law regarding the processing and protection of personal data, the BC 5701 and the requirements established in Section 4.3 and Section 4.4;

b. monitor compliance with:

   1. the requirements of the GDPR;
   2. the established requirements (see: Section 4.3 and Section 4.4);
   3. the requirements of the BC 5701;
   4. the policies on the processing and protection of personal data;

c. monitor the adequate privacy awareness of all employees and parties involved in the processing;

d. provide advice on and monitor the conduct of DPIAs when requested to do so;

e. act as a point of contact for the supervisory authorities on issues relating to the processing of personal data, including the prior consultation referred to in Article 36 GDPR, and to consult, where appropriate, with regard to any other matter;

f. cooperate with the supervisory authorities.

Objective **The DPO shall perform his or her legal tasks taking into account the nature, scope, context and purposes of the processing.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

5.4 Records of the processing activities

5.4.1 Record for the controllers C

The organisation and shall create and maintain a record of the processing activities under its responsibility. The record shall contain at least the following information:

a. the name and contact details of the organisation and the DPO;

b. the processing and, for each processing operation:

   1. the purposes of the processing;
   2. the categories of data subjects;
   3. the categories of personal data;
   4. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
   5. where applicable, the transfer of personal data to a third country or international organisation, including the identification of that third country or international organisation and the documentation relating to the appropriate safeguards;
   6. where possible, the envisaged time limits for erasure of the different categories of data;
   7. where possible, a general description of the technical and organisational security measures relating to the processing.

The register shall be kept in electronic format.

Objective **The organisation shall unambiguously record all processing activities in an electronic record of processing activities for the controller. The record shall be complete, accurate and up-to-date.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

5.4.2 Record for the processors P

The organisation shall create and maintain a record of all categories of processing activities carried out on behalf of controllers and processors. The record shall contain at least the following information:

a. the name and contact details of the organisation and the DPO;

b. the name and contact details of each controller and processor on behalf of which the organisation processes personal data, and, where applicable, the controller's or processor's representative and their DPO;

c. the categories of processing carried out on behalf of each controller or processor;

d. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;

e. where possible, a general description of the technical and organisational security measures relating to the processing.

The register shall be kept in electronic form.

Objective **The organisation shall keep an unambiguous, complete, accurate and up-to-date record in electronic form of all of processing operations it carries out on behalf of controllers and processors.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

6. Fundamentals of the processing activities

6.1 Principles relating to the processing activities C

The organisation shall ensure that it processes personal data in accordance with the principles of Article 5 GDPR.

Objective **The organisation shall establish a framework to ensure that it complies with the principles of Article 5 GDPR when processing personal data.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

6.1.1 Processing purposes C

Personal data shall be collected for specified, explicit and legitimate purposes and shall not be further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or for statistical purposes shall not be considered to be incompatible with the initial purposes, provided that it is determined and documented that the processing qualifies as processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, and the additional requirements regarding appropriate safeguards for the rights and freedoms of the data subject are determined and complied with.

Objective **Processing operations shall be limited to well-defined, clearly described and legitimate purposes and shall not be processed in a way incompatible with those purposes.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

6.1.1.1 Transmission of personal data to a third party C

Where the organisation transmits personal data to a third party that is itself a controller for the processing of those personal data, the organisation shall ensure that the transmission complies with the requirements of the GDPR.

Objective **Any transmission of personal data to one or more third parties shall be lawful, and the data subjects shall be given timely and adequate notice of the transmission.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

6.1.2 Lawfulness C

The organisation shall determine that processing is allowed because one of the following conditions has been met:

a. the data subject has given consent to the processing of their personal data for one or more specific purposes;

b. the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c. the processing is necessary for compliance with a legal obligation to which the organisation is subject;

d. the processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e. the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the organisation;

f. the processing is necessary for the purposes of the legitimate interests pursued by the organisation or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Where the ToE involves the processing of special categories of personal data (Article 9 GDPR) or personal data relating to criminal convictions and offences (Article 10 GDPR), the organisation shall also determine that the prohibition on processing such personal data does not apply to the processing.

Objective **The lawfulness of all processing operations shall be determined correctly and its analysis shall be documented.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

6.1.3 Data minimisation C

The processing of personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Objective **The processing of personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes of the processing.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

6.1.4 Accuracy C

Personal data processed shall be accurate and, where necessary, kept up to date. Every reasonable step shall be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are rectified or erased without delay.

Objective **Personal data processed shall be accurate and up to date.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

6.1.5 Storage limitation C

Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. In particular, this means ensuring that the length of time for which personal data is stored is restricted to the minimum necessary.

Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, provided that appropriate technical and organisational measures are taken to safeguard the rights and freedoms of the data subjects.

Objective **The organisation shall ensure that personal data is erased or anonymised as soon as it is no longer necessary for a lawful processing purpose.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

6.2 Requirements for the processor regarding the principles of the GDPR P

The organisation shall ensure that it complies with the applicable principles of the GDPR when processing personal data on behalf of one or more controllers.

Objective **The organisation shall ensure that it complies with the principles of the GDPR in relation to the personal data it processes under the authority of a controller.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

6.3 Documenting the processing operations C | P

With respect to the ToE the organisation shall:

a. adequately document the related process or processes;

b. adequately document the process steps of the process or processes;

c. document appropriate procedures corresponding to the process steps.

Objective **The processing operations shall be documented consistently and in a manner that is understandable to all relevant parties.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

6.4 Controller and processor C | P

The organisation shall define the role of each party in the chain(s) of processing operations with regard to the processing of personal data.

Objective **The GDPR-role of the parties involved in the processing activities shall be clearly and correctly defined and agreed upon.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

7. Technical and organisational protection

7.1 General C | P

The organisation must select a well-established information security best practice that is appropriate to the risks to the rights and freedoms of data subjects associated with the processing, and comply with it with respect to the scope of BC 5701.

Objective **The organisation shall select, implement and comply with a well-established information security best practice for the adequate protection of the confidentiality, integrity and accuracy of the personal data processed and the resilience of the processing and the processing system.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

7.2 Risk management C | P

The organisation shall establish, implement and maintain a risk management process that at least identifies and lists, assesses, evaluates and manages the risks to the data subjects associated with the processing of their personal data.

The process shall ensure that, in addition to the risks associated with a breach of confidentiality, integrity and availability, and the resilience of the processing and the processing system, the risks to the rights and freedoms of the data subjects arising from the processing itself are taken into account.

Objective **The organisation shall establish a risk management process to consistently identify the risks to the data subjects' rights and freedoms associated with processing and to avoid or mitigate the identified risks appropriately within a clear framework.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

7.2.1 Risk management for processors P

The organisation shall take steps to ensure that it receives adequate instruction regarding the processing and protection of personal data and upon request assist controllers in carrying out a risk analysis in relation to the processing of personal data.

Objective **The organisation shall take appropriate steps to ensure it receives adequate instructions with regard to the protection of the rights and freedoms of data subjects, based on an informed and appropriate risk analysis.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

7.3 Data protection impact assessment (DPIA) C

Whenever the organisation intends to process personal data, the organisation shall assess the impact of the intended processing on the protection of personal data prior to the processing of personal data, and in particular when using new technologies, which by their nature, scope, context and purpose may present a high risk to the rights and freedoms of natural persons.

In particular, a DPIA shall be carried out in the following situations:

a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b. the processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences;
c. systematic monitoring of a publicly accessible area on a large scale.

In addition, the EDPB and the relevant supervisory authorities may provide overviews of processing operations for which a DPIA is or is not required.

Objective **The organisation shall determine whether a DPIA is required for each intended processing operation and for each intended substantial change to an existing processing operation and, if so, shall carry it out appropriately.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

7.3.1 Prior consultation (where applicable) C

Where a DPIA shows that:

a. the processing operations would pose a high risk to the rights and freedoms of natural persons in the absence of safeguards, security measures and risk mitigation measures; and
b. the organisation considers that it is not possible to mitigate that risk by measures that are reasonable in view of the available technology and the cost of implementation,

the organisation shall consult the supervisory authority concerned before commencing the processing.

Objective **Processing operations involving high risk for the rights and freedoms of the data subjects shall be submitted for assessment to the supervisory authority concerned prior to the processing. The recommendations of the supervisory authority shall be followed up before processing starts.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

7.3.2 DPIA for processors P

The organisation shall upon request assist controllers in carrying out DPIAs.

Objective **The organisation shall ensure that any obligations to assist controllers in relation to DPIAs concerning the ToE are fulfilled in a timely manner.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

7.4 Data protection by design and by default C | P

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the organisation shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

The organisation shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Objective **The organisation shall ensure that, where possible, the principles of data protection by design and by default are applied at the design stage of (changes to) processing operations, when outsourcing processing operations and procuring supporting assets.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

7.5 Staff C | P

The organisation shall identify the personnel required for the effective implementation, operation and maintenance of the compliance to the GDPR, the BC 5701 and the chosen information security best practice and shall ensure that they can be entrusted with the tasks to be performed.

Objective **The organisation shall have staff who can be entrusted with the development, operation and maintenance of the processing and protection of personal data.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

7.5.1 Competences C | P

The organisation shall:

a. determine the required competencies of the persons who under its authority perform activities that may affect the organisation's data protection performance;

b. ensure that such persons are competent on the basis of appropriate education, training and experience;

c. systematically review and, where necessary, further develop the competences of staff involved in the processing and protection of personal data.

Objective **The development, operation, support and maintenance of the processing and protection of personal data shall be carried out by competent staff.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

7.5.2 Training and raising awareness C | P

The organisation shall ensure that persons carrying out activities under the authority of the organisation are aware of:

a. the relevant policies regarding the development, operation and maintenance of processing operations and the protection of personal data;

b. their contribution to the effective implementation of the GDPR and the BC 5701;

c. the consequences for the data subjects of failure to comply with the requirements of the GDPR and the BC 5701.

Objective **The internal and external persons involved in the processing and protection of personal data shall be aware of the risks to the data subjects associated with the processing, of their role in managing those risks and, where applicable, be able to inform and assist the data subjects with regard to the processing of their personal data and the exercise of their rights.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8. Operational execution

8.1 Access to data files C | P

The organisation shall ensure that it always has insight into and, where applicable, access to the personal data processed by the organisation or under its authority.

The implementation requirements in this section relate to electronic and paper files, onsite and offsite, production data and backup data, and data within the organisation and with processors, sub-processors and recipients.

Objective **The organisation shall at all times be able to identify the location of, and have access to, the personal data which it processes or which is processed under its responsibility.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.2 Interaction with the data subject

8.2.1 General C

The organisation shall ensure that the data subjects are provided with information about the processing of personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed to a child.

If the organisation carries out processing activities directed at data subjects in more than one Member State, the organisation shall assess whether the legal provisions of the relevant Member States apply that may affect the interaction with the data subjects.

Objective **Any information provided by the organisation to the data subjects about the processing and the risks associated with it shall be relevant, tailored and understandable to the data subjects.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.2.2 Providing information to the data subject C

The organisation shall ensure that adequate information is provided to the data subjects prior to the processing of their personal data.

The information that must be provided and the manner in which it must be provided depends on whether the organisation has obtained the personal data directly from the data subject (Article 13 GDPR) or not (Article 14 GDPR).

Where the organisation has obtained the personal data directly from the data subject and the organisation intends to further process the personal data for a purpose other than that for which the personal data was collected by the organisation, the organisation shall provide the data subject with information about that other purpose and any other relevant information prior to further processing (Article 13(3) GDPR).

Where the organisation has obtained the personal data directly from the data subject, the organisation is not required to inform the data subject where and insofar as the organisation can demonstrate that the data subject already has the required information (Article 13(4) GDPR).

Where the organisation has not obtained the personal data directly from the data subject, the organisation is not required to inform the data subject directly where:

a. and insofar as the organisation can demonstrate that the data subject already has the required information; or

b. the collection or disclosure of the personal data is expressly required by law; or

c. the provision of the information to the data subject is impossible or involves a disproportionate effort; or

d. the personal data must remain confidential for reasons of professional secrecy, including a statutory duty of confidentiality, in accordance with EU or Member State law,

in which case the organisation shall take appropriate measures to protect the rights, freedoms and legitimate interests of the data subjects, including making the information publicly available (Article 14(5)(b) GDPR).

Where the organisation carries out processing operations directed at data subjects in more than one Member State, the organisation shall verify whether there are any legal requirements in these Member States that may affect the information provided to the data subjects.

Objective **The organisation shall provide the data subjects with adequate information about the processing of their personal data prior to the collection or, where applicable, the processing of their personal data.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.2.2.1 The provision of information via the processor *(where applicable)* P

Where the organisation provides services to controllers that involve a user interface with the data subjects, the organisation shall actively assist the controller in fulfilling its obligation to provide information to the data subjects.

Objective **Where applicable, the organisation shall actively assist controllers in complying with the requirements to provide information to data subjects.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.3 Demonstrability of consent

8.3.1 Securing the lawfulness of processing based on consent C

8.3.1.1 Obtaining consent *(where applicable)* C

Where the organisation uses consent as legal basis for the processing, the organisation shall ensure that:

a. the organisation demonstrably obtains the lawful consent of the data subjects prior to the processing;

b. consent is given in an unambiguous affirmative manner that establishes a freely given, specific, informed and clear indication of the data subject's agreement to the processing;

c. where applicable, the lawfulness of the consent of children has been ensured;

d. the consent is kept in its original form;

e. the data subject can withdraw his or her consent at any time in a manner that is as easy as giving consent, in which case the processing shall be terminated without undue delay. The data subject shall be informed of this right before consent is given.

Objective **Where the organisation processes personal data on the basis of the data subject's consent, the organisation shall be able to demonstrate that the consent was lawfully obtained and is valid.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.3.1.2 Consent related to information society services *(where applicable)* C

Where the organisation processes personal data in relation to the offer of information society services directly to a child, the organisation shall ensure that the data subject is at least sixteen years old.

If the data subject is below the age of sixteen, the organisation shall ensure that the consent is given or authorised by the person who holds the parental responsibility over the child.

If the law of a Member State provides for a lower age for parental consent, the organisation shall apply the lower age to the data subjects in that Member State, provided that this age is not lower than thirteen years.

Taking into account available technology, the organisation shall make reasonable efforts to verify that the consent is given or authorised by the holder of parental responsibility over a child below the age limit applicable.

Objective **The organisation shall appropriately determine the age of the data subjects and shall obtain, and be able to demonstrate, lawful consent in relation to offers of information society services directly to children.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.3.2 Securing the lawfulness of processing based on other legal grounds C

Personal data shall be processed lawfully and the organisation shall be able to demonstrate this.

Objective **The organisation shall ensure and be able to demonstrate that the processing is lawful with respect to each individual data subject.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.4 The rights of the data subject

The organisation shall ensure that, where applicable, the following rights of the data subject are adequately respected:

a. the right of access;

b. the right of rectification;

c. the right to erasure;

d. the right to restriction of processing;

e. the right to data portability;

f. the right to object;

g. the right not to be subjected to decisions based solely on automated processing;

h. the notification obligation regarding the rectification or erasure of personal data or the restriction of processing.

Where the purposes for which an organisation processes personal data do not or do no longer require the identification of a data subject, the organisation is not obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with the GDPR.

Where the organisation can demonstrate that it is not in a position to identify the data subject, it shall inform the data subject accordingly, if possible. In such cases, the rights referred to in Sections 8.4.2 to 8.4.7 and 8.4.9 shall not apply, except where the data subject, for the purpose of exercising his or her rights provides additional information enabling his or her identification.

If the organisation cannot, or can no longer, identify a data subject on the basis of the information available and the data subject, in exercising his or her rights, provides additional information that enables him or her to be identified in order to exercise his or her rights, the organisation shall comply with a request from the data subject relating to the rights referred to above.

If the organisation carries out processing activities directed at data subjects in more than one Member State, the organisation shall determine whether any legal exceptions or derogations have been established in the respective Member State's law with respect to the rights of the data subjects (see: 4.3) and shall comply with them when fulfilling the data subjects' requests.

Any communication with the data subject regarding his or her rights shall be in a concise, transparent, intelligible and easily accessible form, using clear and plain language (see: 8.2.1).

8.4.1 Internal assurance C

The organisation shall ensure that, for all processing operations using the personal data of identified or identifiable data subjects, it handles any request from the data subjects to exercise their rights under the GDPR in accordance with the GDPR.

Objective **The organisation shall be able to handle any legitimate and executable request by the data subjects to exercise their rights related to the GDPR demonstrably in a timely and appropriate manner.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.4.1.1 Assisting the controller P

The organisation shall ensure that, where applicable, it assists the controllers in fulfilling their obligations arising from the data subjects' rights.

Objective **The organisation shall, where possible, provide adequate assistance to the controller in exercising the data subjects' rights referred to in Sections 8.4.2 to 8.4.8.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.4.2 The right of access C

Where a data subject requests access to his or her personal data, the organisation shall inform the data subject whether his or her personal data are being processed and, if so, about the processing.

The information shall be provided to the data subject in writing or by electronic means. If the organisation provides the information orally at the request of the data subject, it shall ensure that the identity of the data subject can be established by other means.

Objective **The organisation shall provide any data subject who submits a legitimate and executable request with timely access to his or her personal data being processed, as well as relevant information regarding the processing.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.4.3 The right to rectification C

At the request of the data subject, and taking into account the purposes of the processing, the organisation shall rectify any inaccurate personal data of the data subject, complete incomplete personal data or add supplementary information.

Objective **The organisation shall deal promptly and appropriately with any legitimate and executable request for rectification.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.4.4 The right to erasure C

The organisation shall erase the data subjects' personal data without undue delay upon the data subject's request if:

a. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; or
b. the data subject withdraws the consent on which the processing is based and there is no other legal basis for the processing; or
c. the data subject objects to the processing:
    1. on grounds relating to his or her particular situation, with regard to the processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1) GDPR, including profiling based on those provisions; or
    2. where personal data are processed for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing; or
d. the personal data have been processed unlawfully; or
e. the personal data have to be erased for compliance with a legal obligation under EU or Member State law to which the organisation is subject; or
f. the personal data have been collected in relation to the offer of information society services directly to a child, as referred to in Article 8(1) GDPR.

Objective **The organisation shall deal promptly and appropriately with any valid and executable request for the erasure made by a data subject.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.4.5 The right to restriction of processing C

At the request of the data subject, the organisation shall without undue delay protect the personal data from (further) processing and inform the data subjects before lifting the restriction on processing if:

a. the accuracy of the personal data is contested by the data subject, for a period of time sufficient for the organisation to verify the accuracy of the personal data; or
b. the processing is unlawful and the data subject objects to the erasure of the personal data and requests instead that the use of the personal data is restricted; or
c. the personal data are no longer needed by the organisation for the purposes of the processing but are needed by the data subject for the establishment, exercise or defence of legal claims; or
d. the data subject has objected to the processing in accordance with Article 21 of the GDPR, pending the verification of whether the organisation's legitimate interests override those of the data subject.

Objective **The organisation shall deal promptly and appropriately with any valid and executable request for restriction, and shall inform the data subject before lifting the restriction.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.4.6 The right to data portability C

Where the processing is based on the data subject's consent or on a contract to which the data subject is a party and the processing is carried out by automated means, the organisation shall, upon request, provide the data subject with the personal data previously supplied by the data subject to the organisation in a structured, common and machine-readable form or, where technically feasible, transmit such data directly to another controller without hindrance.

Objective **The organisation shall deal promptly and appropriately with any valid and executable request for data portability.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.4.7 The right to object C

The organisation shall respect the data subject's objection to the processing of his or her personal data if:

a. the data subject objects to the processing of his or her personal data on grounds relating to his or her particular situation and the processing is based on the public interest or the exercise of official authority vested in the organisation (Article 6(1) GDPR under e)), or legitimate interest (Article 6(1) GDPR under f)), unless the organisation demonstrates compelling legitimate grounds for the processing which override the rights and freedoms of the data subject, or which are related to the establishment, exercise or defence of legal claims; or

b. the data subject objects to the processing of personal data for scientific or historical research purposes or scientific purposes on grounds relating to his or her particular situation, unless the processing is necessary for the performance of a task carried out in the public interest; or

c. the processing of personal data for the purpose of direct marketing, including the creation of profiles for direct marketing purposes.

The organisation shall explicitly refer to the right to object and present it clearly and separately from any other information (see also: 8.2.2.b).

Objective **The organisation shall deal promptly and appropriately with any valid and executable objection to the processing of personal data.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.4.8 The right regarding automated decision-making, including profiling *(where applicable)* C

The organisation shall respect the request of data subjects not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, unless the organisation can demonstrate that the processing is:

a. necessary for entering into, or the performance of, a contract between the data subject and the organisation; or

b. permitted by EU or Member State law that applies to the organisation and which lays down appropriate measures to safeguard the data subject's rights and freedoms and legitimate interests; or

c. based on the data subject's explicit consent.

Objective 1 **The organisation shall inform data subjects about the decision-making process and provide them with simple means to object, express their views or request human intervention.**

Objective 2 **The organisation shall ensure that automated individual decision making, including profiling, is systematically assessed for bias.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.4.9 Notification obligation *(where applicable)* C

The organisation shall notify each recipient of personal data of any valid and executable request by a data subject for rectification, erasure of personal data or restriction of processing, unless this proves impossible or involves a disproportionate effort.

Where the organisation has made personal data public, it shall take reasonable steps, taking into account the available technology and the cost of implementation, to notify the controllers who process the personal data of any request for rectification, erasure of personal data or restriction of the processing.

The organisation shall, upon request, provide the data subject with information about these recipients.

Objective **The organisation shall, without undue delay and in a concise manner, inform any recipient of personal data of the exercise of the relevant rights of the data subjects and, upon request, inform data subjects of the recipients of their personal data.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.4.10 Excessive requests C

The organisation shall handle requests from data subjects regarding to their GDPR rights, free of charge.

Where requests from a data subject are manifestly unfounded or excessive, in particular, because of their repetitive nature, the organisation may either:

a. charge a reasonable fee, taking into account the administrative costs of providing the information or communicating, or taking the action requested; or

b. refuse to comply with the request.

When the organisation charges a fee or refuses to comply it shall provide evidence that the request is manifestly unfounded or excessive.

Objective **The organisation shall ensure that it handles all requests from data subjects regarding the processing of their personal data free of charge, unless a request is manifestly unfounded or excessive.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.4.11 Complaints procedure C

The organisation shall ensure that complaints addressed to the organisation by data subjects regarding the processing of personal data are dealt with appropriately.

The complaints procedure shall be publicly available.

Objective **The organisation shall provide adequate information to the data subjects on how to lodge a complaint with the organisation regarding the processing of their personal data and shall handle complaints in an independent and timely manner.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.5 Outsourcing processing activities C | P

If the organisation intends to outsource (part of) a processing operation to a processor, the organisation shall only engage processors that offer sufficient guarantees regarding the technical and organisational measures taken so that the processing operations meet the requirements of the organisation, the GDPR and the BC 5701, and ensure adequate protection of the rights of the data subjects.

Objective **The organisation shall ensure that the processors it engages meet the requirements of the GDPR, the BC 5701 and the organisation in relation to the processing and protection of the personal data.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.5.1 Conformity by processors C | P

The organisation shall ensure that processing operations carried out by processors under the authority of the organisation are carried out in accordance with the requirements of the GDPR and the BC 5701.

Objective **Taking into account the risks to the data subjects associated with the processing operations, the organisation shall ensure that the processors it employs continue to comply with the requirements of the GDPR and the BC 5701 in relation to the processing and protection of personal data.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.6 Processing under the authority of a controller P

The organisation shall ensure that all processing operations under the authority of a controller are carried out in accordance with the instructions of the controller.

Where the organisation acts or may act as a sub-processor in relation to the ToE, the organisation must be aware that it may receive requests for assistance from data controllers with whom the organisation does not have a direct processing relationship, but which it must comply with.

Objective **The processing of personal data shall only be carried out on behalf of and in accordance with the instructions of a competent controller.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.7 International transfer of personal data C | P

When transferring personal data to countries outside the EEA or to an international organisation, the organisation shall ensure that the transfer is lawful by complying with one of the following transfer instruments.

1. Adequacy decision

The European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection (adequacy decision).

2. Appropriate safeguards

In the absence of an adequacy decision, the organisation may transfer personal data to a third country or an international organisation if enforceable data subject rights and effective legal remedies for data subjects are available and the organisation provides one of the next appropriate safeguards.

a. a legally binding and enforceable instrument between public authorities or bodies;

b. binding corporate rules in accordance with Article 47 GDPR;

c. standard data protection clauses adopted by the European Commission in accordance with the examination procedure referred to in Article 93(2) GDPR;

d. standard data protection clauses adopted by a supervisory authority and approved by the European Commission pursuant to the examination procedure referred to in Article 93(2) GDPR;

e. an approved code of conduct pursuant to Article 40 GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

f. an approved certification mechanism pursuant to Article 42 GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

g. authorisation from the competent supervisory authority for contractual clauses between the organisation and the controller, processor or the recipient of the personal data in the third country or international organisation; or

h. with the authorisation from the competent supervisory authority for provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

3. Derogations for specific situations

In the absence of an adequacy decision pursuant to Article 45(3) GDPR, or of appropriate safeguards pursuant to Article 46 GDPR, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

a. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

b. the transfer is necessary for the performance of a contract between the data subject and the organisation or the implementation of pre-contractual measures taken at the data subject's request;

c. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the organisation and another natural or legal person;

d. the transfer is necessary for important reasons of public interest;

e. the transfer is necessary for the establishment, exercise or defence of legal claims;

f. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46 GDPR, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph are applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the organisation which are not overridden by the interests or rights and freedoms of the data subject, and the organisation has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The organisation shall inform the supervisory authority of the transfer. The organisation shall, in addition to providing the information referred to in Articles 13 and 14 GDPR, inform the data subject of the transfer and of the compelling legitimate interests pursued.

International transfers pursuant to a court judgement or decision of an administrative authority of a third country, in accordance with Article 48 GDPR, may take place only if the judgement or decision is based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the EU or a Member State.

If the Member State in which the organisation is located has expressly set limits on the transfer of specific categories of personal data, the organisation shall apply those limits.

Objective **When personal data is transferred to countries outside the EEA or to organisations with establishments outside the EEA, the adequate protection of personal data shall be demonstrably ensured.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.8 Personal data breach

8.8.1 Handling personal data breaches C | P

Where possible and feasible, the organisation shall actively monitor security incidents affecting the availability, integrity, and confidentiality of personal data (incidents), breaches of personal data (data breaches), and the existence of vulnerabilities affecting the protection of personal data, and address them in a thorough and structured manner.

Objective **The organisation shall respond quickly and effectively to (potential) incidents, personal data breaches and reported vulnerabilities affecting the protection of personal data.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.8.2 Notification to the supervisory authority C

In the event of a personal data breach, the organisation shall notify the personal data breach to the supervisory authority concerned without undue delay and no later than 72 hours after becoming aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

If and to the extent that it is not possible to provide all the necessary information at once, it may be provided in phases without undue further delay.

Objective **The supervisory authority concerned shall be informed in a timely and appropriate manner of personal data protection incidents that may result in a risk to data subjects.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.8.3 Notification to the data subject C

Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the organisation shall notify the data subject about the personal data breach without undue delay.

Notification is not required if:

a. the organisation has implemented appropriate technical and organisational security measures, and those measures have been applied to the personal data affected by the personal data breach, in particular, those rendering the personal data unintelligible to any person who is not authorised to access it;

b. the organisation has taken subsequent measures to ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;

c. the notification would require a disproportionate effort, in which case a public notice or similar measure shall be used to inform the data subjects in an equally effective manner.

Objective **Data subjects shall be adequately informed as soon as possible of any data breach that is likely to result in a high risk to their rights and freedoms.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.8.4 Notification to the controller P

As soon as the organisation has become aware of a data breach, it shall notify the controller of the data breach without undue delay.

If, and to the extent that, it is not possible to provide all the necessary information at once, it may be provided in phases without undue further delay.

Objective **Controllers shall be adequately informed of any data breach as soon as possible and shall be adequately assisted in dealing with the breach.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

8.9 Changes in the context of the ToE C | P

Where the organisation identifies changes in the context of the ToE, it shall implement these changes systematically. In doing so, the organisation shall take into account the principles of data protection by design and data protection by default (see: Section 7.4).

With regard to the changes, the organisation shall determine:

a. the purpose of the changes and the potential impact on the processing and protection of personal data;

b. the impact of the changes on the use of resources;

c. the allocation or reallocation of responsibilities and authorities;

and ensuring that:

d. the relevant changes in the processing are communicated to the data subjects and controllers in a timely manner.

Objective **The processing and protection of personal data shall remain sufficient and adequate when the facts and circumstances relating to the processing change.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

9. Management system

9.1 General C | P

The organisation shall establish, document, implement and maintain a management system regarding to the protection of the rights and freedoms of data subjects when processing their personal data.

Objective **The activities of the organisation related to the processing and protection of personal data shall be controlled and continually improved.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

9.2 Documented information

9.2.1 General C | P

The organisation shall at least manage the following documents:

a. the documented information required by the BC 5701;

b. the documented information on which the organisation has based its conclusions regarding the processing and protection of personal data.

Note *The form and content of the documented information will depend on the size and complexity of the organisation, the nature of its activities and the competence of its staff.*

Objective **The documentation relating to the processing and protection of personal data and the management system shall be unambiguous, adequate, fit for purpose and managed.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

9.2.2 Creating and updating C | P

The organisation shall ensure that the documentation to support the processing and protection of personal data and the management system are adequate to support the intended purpose.

Objective **The documented information supporting the processing and protection of personal data and the management system shall be appropriate, adequate and demonstrably up to date, and its management shall be ensured.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

9.2.3 Managing the documented information C | P

Documented information required by the BC 5701 and the management system shall be managed to ensure that:

a. the information is available and suitable for use, where and when it is needed;

b. the information is adequately protected (e.g., against loss of confidentiality, inappropriate use and unauthorised changes).

Objective **The integrity, availability and confidentiality of the documented information supporting the processing and protection of personal data and the management system shall be maintained and the latest version shall be readily available to the relevant persons.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

9.3 Monitoring, measuring, analysing and evaluating C | P

The organisation shall determine:

a. what will be monitored and measured;

b. who sets the targets;

c. the methods of monitoring, measurement, analysis and evaluation required to obtain valid results;

d. when to monitor and measure;

e. who will monitor and measure;

f. when the results of monitoring and measurement will be analysed and evaluated;

g. who will analyse and evaluate the results.

Objective **The organisation shall have ongoing insight into its performance with respect to the processing and protection of personal data and the management system.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

9.4 Internal audit C | P

The organisation shall conduct internal audits at regularly scheduled intervals to determine whether all activities related to the GDPR and the BC 5701 are implemented and being operated in accordance with their design and are being kept up to date.

Objective **The organisation shall systematically obtain objective information on the extent to which all technical and organisational measures related to the processing and protection of personal data are implemented and carried out as designed and are effective.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

9.5 Management review C | P

The Board shall, at planned intervals, assess the organisation's processing and protection of personal data and the management system to ensure its continual suitability, adequacy and effectiveness.

Objective **The Board shall demonstrate leadership and support for the adequate processing and protection of personal data and the management system.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

9.6 Nonconformities and actions C | P

The organisation shall ensure that it takes action to correct and prevent a recurrence of identified nonconformities with regard to the GDPR and the BC 5701.

Nonconformities shall include at least:

a. data protection incidents, including personal data breaches;

b. nonconformities arising from audits;

c. complaints from data subjects or controllers;

Actions shall be proportionate to the impact of the nonconformities.

Objective **The organisation shall address all identified nonconformities relating to the processing and protection of personal data and the management system, correcting them where necessary and shall ensure that they do not recur.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

9.7 Continual improvement C | P

The organisation shall endeavour, where possible and feasible, to continually improve the protection of the rights and freedoms of data subjects when processing their personal data.

Objective **The organisation shall continually improve the suitability, adequacy and effectiveness of the processing and protection of personal data and the management system.**

Implementation requirements

Due to the informative purpose of this document, the further content of this paragraph has been omitted.

Appendix 1 Overview of documentation requirements (informative)

Due to the informative purpose of this document, the content of this appendix has been omitted.

Appendix 2 Cross-reference table GDPR to certification objectives (informative)

Due to the informative purpose of this document, the content of this appendix has been omitted.

Appendix 3 Relevant EDPB guidelines (informative)

Due to the informative purpose of this document, the content of this appendix has been omitted.

Brand Compliance is a European certification body specialising in privacy, information security and quality audits. It is recognised for its expertise and clear, personal approach. Through certification, Brand Compliance confirms the trustworthiness of its clients.

Brand Compliance B.V.

Hambakenwetering 8D2
5231 DC ‘s Hertogenbosch
The Netherlands

+31 (0) 73 220 2000
info@brandcompliance.com
www.brandcompliance.com

Brand Compliance Belgium B.V.

Uitbreidingstraat 66
2600 Berchem (Antwerpen)
Belgium

+32 (0) 14 48 0730
info@brandcompliance.com
www.brandcompliance.com

Brand Compliance Nordics AB

Vasagatan 16
SE-111 20 Stockholm
Sweden

+46 73 157 7805
info@brandcompliance.com
www.brandcompliance.se