TECHNICAL STANDARD

related to personal data protection in complaince with regulation (EU) 2016/679

BUREAU VERITAS CERTIFICATION HOLDING
Le Triangle de l'Arche - 8, Cours du Triangle, CS 90096
92937 Paris la Défense Cedex - France

BUREAU VERITAS

Contents

Foreword

The Regulation (EU) 2016-679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, adopted on April 27th, 2016 and published in the OJEU on May 4th, 2016 (hereinafter referred to as «The Regulation") is intended to modernize the European framework for the protection of personal data in order to take account of technological advances.

Since the Community Directive of October 24th, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, technologies have evolved, leading to an exponential increase in the processing and sharing of personal data.

Hence reducing legal discrepancies between the different legislations of the Member States of the European Union becomes of paramount importance, which is the objective of the Regulation, which will be directly applicable in the Member States of the European Union on May 25th, 2018.

In this perspective and within the framework of their compliance policy, companies must include in their strategy:

- the obligations arising from the Regulation;
- the necessary implementation of actions to comply with these new requirements and within the imposed deadlines.

The regulation requires organizations to assume full liability for the data they control or process, so that they must define related processes and allocate internal resources and skills to ensure optimal personal data protection (the principle of accountability).

Demonstrating that the processing operations carried out by data controllers or processors and their subcontractors and service suppliers comply with the Regulation constitutes a key challenge for companies in terms of brand reputation and image, the penalties that may be incurred as well as in terms of competitiveness.

Hence the development of this certification scheme has been intiated to enable companies to demonstrate their compliance with these new obligations.

The purpose of this certification scheme is to define the technical, organizational and documentary provisions related to accountability requirements as defined in the Regulation: Accountability is a new principle of liability which requires companies to be able to justify all the control and monitoring system set up to ensure personal data protection compliance.

In particular, it involves:

- the obligation to document the requirements for compliance with the various obligations imposed by the Regulation;
- the establishment of technical and organizational measures to ensure compliance and its maintenance in operational conditions;
- the duty to provide evidence of compliance with the Regulation.

1. Scope

According to the Regulation (EU) 2016/679, adherence to approved codes of conduct (Article 40) or approved certification mechanisms (Article 42) may be used as an element by which to demonstrate compliance with the obligations of data controllers and data processors.

In addition to adherence by data controllers or data processors subject to this Regulation, data protection certification mechanisms may be established for the purpose of demonstrating the existence of appropriate safeguards provided by data controllers or data processors that are not subject to this Regulation within the framework of personal data transfers to third countries or international organizations.

Any certification against this certification scheme does not reduce the responsibility of the data controller or the data processor to comply with the Regulation (EU) 2016/679 and is without prejudice to the tasks and powers of the supervisory authorities (Data Protection Authorities).

This certification scheme specifies the requirements related to personal data protection that an organization can implement to achieve compliance with the Regulation (EU) 2016/679.

This technical standard is applicable to any organization, regardless of size, type and nature, and applies to its activities, products and services involving personal data processing, that the organization can control or influence considering a life cycle perspective.

In particular this certification scheme is applicable to any data controller or data processor whatever the nature, scope, context or purposes of personal data processing. For data processors some clauses may be not applicable (see appendix 3). In case a clause is applicable for both data controller and data processor the word organization is used.

In this standard, the following verbal forms are used:

- "shall" indicates a requirement;
- "should" indicates a recommendation;
- "may" indicates a permission;
- "can" indicates a possibility or a capability.

Information marked as "NOTE" is intended to assist the understanding or use of the document.

2. References

The following documents, in whole or in part, have been used as key inputs to develop this certification scheme. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
- WP29 - Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679;
- WP29 - Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679;
- WP29 - Guidelines on Personal data breach notification under Regulation 2016/679;
- WP29 - Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679;
- WP29 - Guidelines on Data Protection Officers ('DPOs');
- WP29 - Guidelines for identifying a controller or processor's lead supervisory authority;
- WP29 - Guidelines on the right to data portability;
- WP29 - Guidelines on consent under Regulation 2016/679;
- WP29 - Guidelines on the right to «data portability»;
- WP29 - Guidelines on transparency under Regulation 2016/679;
- ISO 27001:2013, Information technology -- Security techniques -- Information security management systems -- Requirements»;
- ISO/IEC 29100:2011, Information technology -- Security techniques -- Privacy;
- ISO/IEC 29101:2013, Information technology -- Security techniques -- Privacy architecture framework;
- ISO 9001:2015, Quality management systems - Requirements;

The following documents, in whole or in part, have been used to ensure compliance of this certification scheme to accreditation requirements:

- EDPB - Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679;
- ISO 17065:2012 – Conformity assessment – Requirements for bodies certifying products, processes and services;
- EA 1/22 A:2016 – EA Procedure and Criteria For the Evaluation of Conformity Assessment Schemes by EA Accreditation Body Member.

3. Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1 Management system

Set of interrelated or interacting elements of an organization to establish policies and objectives, and processes to achieve those objectives.

3.2 Organization

Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.

3.3 Top management

Person or group of people who directs and controls an organization at the highest level.

3.4 Rights of the data subject

Refer to articles 12 to 23 (chapter III: rights of the data subjects) of Regulation (EU) 2016/679.

3.5 Compliance obligations

Legal requirements that an organization (3.2) has to comply with and other requirements that an organization has to or may choose to comply with. Compliance obligations are related to personal data protection as per Regulation (EU) 2016/679.

3.6 Process

Set of interrelated or interacting activities that use inputs to deliver an intended result.

3.7 Personal data

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.8 Sensitive personal data

Any personal information related to the individual's:

- racial or ethnic origin;
- political opinions;
- religion or philosophical beliefs;
- trade union membership;
- genetic data;
- health;
- biometric data for the purpose of a unique identification or authentication of a natural person;
- sexual life;
- criminal convictions and offences or related security measures.

3.9 High risk personal data

High risk personal data can include:

- sensitive personal data (3.8);
- personal data of vulnerable natural persons, in particular of children;
- personal aspects evaluated, in particular analyzing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, in order to create or use personal profiles;
- processing involving a large amount of personal data and affecting a large number of data subjects.

The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

3.10 Processing

Any operation or set of operations which is performed on personal data (3.7) or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.11 Controller

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

3.12 Processor

A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (3.11).

3.13 Recipient

A natural or legal person, public authority, agency or another body to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

3.14 Consent of the data subject

Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

3.15 Personal data breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3.16 Supervisory authority/Data Protection Authority

An independent public authority which is established by a Member State pursuant to Article 51 of European regulation 2016/679.

3.17 Accountability

Permanent and dynamic process that consists both of an obligation to be accountable with regard to compliance with statutory and regulatory requirements and of a mechanism that is able to demonstrate the efficiency of measures taken and the effectiveness of data protection.

3.18 Data Protection Impact Assessment

Data Protection Impact Assessment (DPIA) is a process which assists organizations (controllers) in identifying, assessing and minimizing the risks (related to the rights and freedoms to the data subjects) of products or services and the actions to be carried out.

3.19 Data protection by design

Each new service or business process that makes use of personal data must take the protection of such data into consideration. An organization needs to be able to show that they have adequate security in place and that compliance is monitored. In practice this means that personal data aspects shall be taken into account during the whole life cycle of the system or process development.

3.20 Data protection by default

Obligation to make sure that, by default, the functionalities of files and applications with personal data ensure a high level of data protection: the strictest privacy settings automatically apply once a customer acquires a new product or service. In other words, no manual change to the privacy settings should be required on the part of the user. There is also a temporal element to this principle, as personal information must by default only be kept for the amount of time necessary to provide the product or service.

3.21 Binding Corporate Rules

Personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

3.22 Life cycle

Consecutive and interlinked stages of a product (or service) system, from design/development phase to final disposal.

3.23 Infrastructure

Organization system of facilities, equipment and services needed for the operation of an organization.

4. Organization and Structure

4.1 Leadership and commitment

Top management shall demonstrate it is fully committed to the implementation of the requirements of this certification scheme and to processes which ensure compliance of data processing with Regulation (EU) 2016/679.

Top management shall implement technical and organizational measures to ensure and demonstrate that the processing of personal data complies with the principles relating to processing of personal data as expressed in article 5 of Regulation (EU) 2016/679.

In particular these measures must:

a) be linked to the nature, scope, context and purposes of the processing;
b) be adapted to the risks of likelihood and severity for the rights and freedoms of natural persons;
c) be applied to all processing activities throughout the lifecycle of products or services starting from the design development of products and/or services involving personal data processing.

These measures shall be evaluated at regular intervals and updated if necessary.

4.2 Policy

4.2.1 Establishing the personal data protection policy

Top management shall establish, document, implement and maintain a policy which states its commitment to deliver products and/or services involving personal data processing in compliance with Regulation (EU) 2016/679 and its accountability to customers and data subjects.

This policy shall include a commitment

a) to the protection of personal data, including prevention of personal data breaches;
b) to fulfil its compliance obligations (see 5.2);
c) to implement technical and organizational measures within the organization to ensure compliance with Regulation (EU) 2016/679.

4.2.2 Communicating the personal data protection policy

This policy shall be:

- available, communicated, understood and applied within the organization including subcontractors and service suppliers if needed;
- available to relevant interested parties, as appropriate.

4.3 Organizational roles, responsibilities and authorities

4.3.1 Organization and responsibilities

The organization shall have a documented organizational structure to ensure compliance with Regulation (EU) 2016/679 (see 5.2).

The responsibilities and authorities related to personal data processing shall be identified, assigned and understood as well as resources identified and allocated.

4.3.2 Data Protection Officer

A Data Protection Officer shall be appointed to ensure compliance of processes related to personal data protection.

The Data Protection Officer shall be designated on the basis of professional skills, experience and knowledge of data protection law and practices.

The organization shall ensure that the Data Protection Officer is involved, in all issues related to the protection of personal data and shall allocate appropriate budget and resources to fulfil his/her tasks.

The Data Protection Officer shall report to the highest level of the organization.

The organization shall ensure that the Data Protection Officer can exercise his/her tasks with necessary independence and confidentiality. In case the Data Protection Officer is in charge of other tasks it shall not result in a conflict of interest.

The Data Protection Officer shall perform the following tasks:

a) inform and advise the organization and the employees who carry out personal data processing of their obligations (see 5.2);
b) monitor compliance of the organization with the compliance obligations (see 5.2) and internal policies and provisions including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
c) organize the conduct of periodic reviews of the set of technical and organizational measures related to personal data protection (see 6.7);
d) provide advice where requested with regard to the Data Protection Impact Assessment and monitor its performance;
e) co-operate with the Supervisory Authority;
f) act as the contact point for the Supervisory Authority on issues relating to personal data, where appropriate.

The organization shall communicate the contact details of the Data Protection Officer to Supervisory Authority and other stakeholders whenever required.

NOTE: The Data Protection Officer can be an employee or a contracted person. Professional skills and experience shall cover both management skills, IT/IS aspects and knowledge of the organization's products and services.

NOTE: The article 29 Guidelines on Data Protection Officers ('DPOs') can be used to identify and mitigate potential situation of conflict of interest.

5. Personal Data Risk Management

5.1 General

The organization shall implement an effective plan related to personal data protection considering the nature, scope, context and purposes of processing and associated risks.

This action plan shall address:

a) compliance obligations (see 5.2);
b) outcomes of Data Protection Impact Assessments (see 5.3);
c) measures to monitor and control the effectiveness.

When planning these actions, the organization shall:

- consider the technological state of the art and its financial, operational and business requirements;
- evaluate the effectiveness of these actions by choosing technical measures adapted to the risks identified.

5.2 Compliance obligations

The organization shall determine all compliance obligations related to personal data processing operations including:

a) Regulatory requirements: Regulation (EU) 2016/679, and any other Union or Member State data protection provisions;
b) Imposed codes of conduct or binding corporate rules;
c) Data controller or specific customer policies and requirements related to personal data protection.

The organization shall take these compliance obligations into account when establishing, implementing, maintaining and continually improving its set of technical and organizational measures and maintain documented information about its compliance obligations.

5.3 Data Protection Impact Assessment (DPIA)

The data controller shall determine the activities, products and services involving personal data processing that can affect the confidentiality and integrity of personal data and potential situations of personal data breaches considering a life cycle perspective (see 7.3).

The data controller shall define a procedure and criteria for DPIA performance. These criteria shall take into account the technological state of the art and the nature, scope, context and purposes of the processing resulting in a high risk to the rights and freedoms of natural persons in accordance with article 35 of Regulation (EU) 2016/679.

The data controller with the support of data processors shall take into account:

a) a systematic description of the processing operations and the purposes of the processing (see 7.3);
b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
c) an assessment of the risks to the rights and freedoms of data subjects;
d) the risk category of personal data;
e) abnormal conditions and reasonably foreseeable situations that may lead to personal data breaches;

f) the measures to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate regulatory compliance taking into account the rights and legitimate interests of data subjects and other persons concerned;
g) any change of the risk represented by processing operations, including planned or new developments, and new or modified activities, products and services.

This data Protection Impact Assessement shall be developed and managed through a multi-disciplinary approach that includes marketing, commercial or business development, operations, information technology and security, legal and other relevant functions including views of data subjects or their representatives, if appropriate; particular advice from the Data Protection Officer shall be sought.

The Data Protection Impact Assessment shall be documented including potential situations of personal data breaches.

The data controller shall communicate the outputs of the Data Protection Impact Assessment to the relevant levels and functions of the organization including the data processors, as appropriate.

5.4 Managing Personal Data Breaches

The organization shall establish, implement and maintain the process(es) needed to prepare for and respond to potential personal data breach situations (see 5.3).

Notably, the organization shall:
a) prepare to respond by planning actions to prevent or mitigate personal data breaches and their consequences, appropriately to the magnitude of breaches and their potential impact;
b) respond to actual data breach situations;
c) periodically test the planned response actions, where practicable;
d) periodically review and revise the process(es) and planned response actions, in particular after the occurrence of personal data breach situations or tests;
e) provide relevant information and training related to personal data breach preparedness and respond, as appropriate, to relevant interested parties, including persons working under its control.

The data processor shall notify the data controller without undue delay after becoming aware of a personal data breach.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall communicate the personal data breach to the data subject without undue delay.

In addition, in case of a personal data breach, the data controller shall, without undue delay, notify the Supervisory Authority about the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The communication to the data subject and/or to the Supervisory Authority shall meet requirements expressed in articles 33 and 34 of Regulation (EU) 2016/679.

The organization shall maintain records of any data breaches comprising the facts relating to the personal data breach, its effects and the remedial action taken. These records shall be made available to the Supervisory Authority on request.

6. Management System

6.1 Manual and procedures

The organization shall establish, implement, maintain and continually improve a set of processes and procedures ("management system") in accordance with the following elements of this certification scheme, which ensure correct implementation and maintenance of personal data related process(es). The "management system" shall be appropriate to the type, range and volume of products and/or services involving personal data processing and associated risks of likelihood and severity for rights and freedoms of natural persons.

This "management system" shall support the organization's business processes, and their interactions, ensuring that the personal data are collected, processed and stored or archived in a compliant manner including appropriate security of the personal data, protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

NOTE: Quality management system (ISO 9001:2015) standard or information security management system (ISO 27001:2013) standard may be used to meet the minimum requirements for the management system defined in this certification scheme.

6.2 Documented information

The organization's "management system" shall include documented information related to data processing and to personal data protection process(es).

The organization shall have a procedure to manage documented information, including appropriate:

- identification, description, review and approval;
- distribution, access, rectification, deletion and use;
- storage and preservation;
- control of changes;
- retention and disposal.

The organization shall maintain records to demonstrate the effective control of products and/or services compliance.

Records shall be legible, maintained in good condition, retrievable and retained for a defined period with consideration given to relevant legal or customer requirements.

6.3 Performance evaluation

The organization shall determine:

a) what needs to be controlled and monitored, and when;
b) the methods for monitoring, measurement, analysis and evaluation;
c) the performance criteria and appropriate indicators.

In addition, the organization shall establish, implement and maintain the process(es) needed to evaluate fulfilment of its compliance obligations (see 5.2).

The organization shall retain documented information as evidence of the monitoring and compliance of its operations.

6.4 Internal audit

The organization shall conduct internal audits at least annually covering all requirements of this certification scheme to provide information on whether:

- it conforms to the requirements;
- it is effectively implemented and maintained.

The scope and frequency of the audits shall take into consideration the risks to personal data processes and activities and previous audit performance.
Internal audits shall be carried out by appropriately trained, competent auditors. Impartiality of auditors shall be ensured.

Audit reports shall detail any significant deviation from requirements of this standard. In particular, audit reports shall identify issues related to technology or processes which could affect the compliance obligations (see 5.2).

6.5 Nonconformity and corrective action

The organization shall determine opportunities for improvement and implement necessary actions to meet compliance obligations (see 5.2) and prevent recurrence.

When a nonconformity occurs, the organization shall:

a) take action to address the immediate issue;
b) evaluate actions through the identification of a root cause of a nonconformity to prevent recurrence elsewhere;
c) implement the action plan, verify that the corrections have been effectively implemented.

The organization shall retain documented information as evidence of the nature of the nonconformities and the related corrective actions.

6.6 Complaints

The organization shall ensure that complaints from customers and interested parties are effectively managed.

The organization shall publically communicate about the process to manage complaints.

Upon receipt of the complaint, the organization shall:

a) acknowledge the complaint to the complainant;
b) gather and verify all necessary information to evaluate and validate the complaint and make a decision on the complaint;
c) formally communicate the decision on the complaint to the complainant;
d) ensure that any appropriate corrective and preventive actions are taken.

6.7 Management review

The Data Protection Officer shall organize management reviews attended by top management at appropriate planned intervals, annually as a minimum, to review the performance of the organization related to personal data protection.

The management review shall include the following topics; as appropriate:

- status of previous management review action plans;
- results of internal and external audits;
- customer satisfaction and/or feedback from interested parties including complaints;
- incidents, breaches, nonconformities and associated corrective actions;
- the effectiveness of actions taken to address the Data Protection Impact Assessments; monitoring and surveillance results;
- performance of suppliers and service providers;
- any change in compliance obligations.

The outputs of the management review shall include:

- opportunities for improvement;
- an action plan including resource needs;
- improvement actions, if needed, when data protection compliance has not been achieved;
- any implication for the personal data protection policy of the organization.

Conclusion of management reviews and associated action plans shall be effectively communicated to appropriate staff, and implemented. Records of the management reviews shall be documented.

6.8 Communication

6.8.1 General

When establishing its communication process(es), the organization shall:

a) take into account its compliance obligations (see 5.2);
b) ensure that information communicated related to personal data protection is consistent with the requirements of this standard, and is reliable.

The organization shall retain documented information as evidence of its communication, as appropriate.

6.8.2 Internal communication

The organization shall:

a) internally communicate information relevant to the data protection management system among the various levels and functions of the organization, including changes to the management system, as appropriate;
b) ensure its communication process(es) enable(s) persons doing work under the organization's control to contribute to continual improvement.

The organization shall ensure that any customer-specific policies or requirements, codes of conduct, binding corporate rules etc. are understood, implemented and clearly communicated to relevant staff and, where appropriate, suppliers and service providers.

6.8.3 External communication

The organization shall externally communicate information relevant to personal data protection, as established by the organization's communication process(es) and as required by its compliance obligations (see 5.2).

In particular, data controllers with the support of data processors shall take appropriate measures to provide any information to data subject related to the rights and freedoms of natural persons, according to articles 12 to 23 (chapter III: rights of the data subjects) of Regulation (EU) 2016/679.

7. Product and/or service control

7.1 Requirements for products and services

The organization shall ensure that the requirements for products and/or services are defined including:

a) compliance obligations (see 5.2)

b) internal requirements considered necessary by the organization or imposed by codes of conduct or binding corporate rules.

The organization shall conduct a review of its ability to meet the requirements for products and/or services to be offered to customers.

The organization shall retain documented information, as applicable, on the results of this review. This review shall be updated in case of any change of requirements for the products and/or services.

7.2 Design and development of products and/or services

The data controller shall establish, implement and maintain a design and development process which ensures continuous compliance of data processing all along the life cycle of products and/or services including end-of-life treatment and final disposal of its products and/or services.

The data controller with the support of data processors shall implement appropriate technical and organizational measures for ensuring that:

- these requirements for products and services are taken into consideration for design and development;
- the personal data processing complies with the principles relating to processing of personal data as expressed in article 5 of Regulation (EU) 2016/679;
- processing complies with the interests or fundamental rights and freedoms of the data subject or any natural person, and, in particular, of vulnerable persons, including children:
- appropriate security measures related to personal data are defined in accordance with article 32 of Regulation (EU) 2016/679;
- outcomes of the related Data Protection Impact Assessment have been taken into account and, in particular, consequences of failure due to the nature of the products and services (see 5.3);
- 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;
- the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

The data controller shall control the design and development process to ensure that the resulting products and services meet the requirements for the specified application or intended use.

Design and development of products or services shall only be validated after a review of appropriate closure of noncompliances related to personal data protection.

The data controller shall retain documented information related to design and development activities.

NOTE: Rights and freedoms of natural person are expressed in articles 12 to 23 (chapter III: rights of the data subjects) of Regulation (EU) 2016/679.

7.3 Release of products and/or services

Where products and/or services involving personal data processing require positive release, procedures shall be in place to ensure that release does not occur until all release requirements have been completed and release authorized.

In accordance with article 30 of Regulation (EU) 2016/679, the organization shall maintain records of processing activities under its responsibility (hard or electronic forms).

This record shall contain the following information (at data controller level):

a) name and contact details of the data controller and the Data Protection Officer;
b) the purposes of the processing;
c) a description of the categories of data subjects and of the categories of personal data;
d) the categories of recipients;
e) where applicable, transfers of personal data to a third country or an international organization;
f) where possible, the envisaged time limits for erasure of the different categories of data;
g) where possible, a general description of technical and organizational measures related to security of personal data.

This record shall contain the following information (at data processor level):

a) name and contact details of the data processor;
b) the categories of the processing carried out on behalf of each controller;
c) where applicable, transfers of personal data to a third country or an international organization;
d) where possible, a general description of technical and organizational measures related to security of personal data.

The organization shall make the records available to the Supervisory Authority on request.

8. Operational control

The organization shall develop, implement and maintain documented procedures and/or instructions that ensure the compliance of its processing operations including its supply chain.

8.1 Processing control

Personal data shall be

a) processed lawfully, fairly and in a transparent manner in relation to the data subject;
b) accurate, and where necessary, kept up to date;
c) kept in a form that permits identification of data subjects for no longer than is necessary for the purposes;
d) processed in a manner that ensures appropriate security of the personal data.

Personal data processing shall be operated in compliance to the rights and freedoms of natural person as expressed in articles 12 to 23 (chapter III: rights of the data subjects) of Regulation (EU) 2016/679 in particular the rights related to

- information and access to personal data;
- right of access by the data subject;
- right to rectification;
- right to erasure;
- right to data portability;
- right to object.

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the organization shall implement appropriate technical and organizational measures to control the processing and to be able to demonstrate that processing is performed in compliance with applicable compliance obligations (see 5.2).

Procedures and/or instructions shall be available and specify how personal data are processed in compliance with principles expressed in article 5 of Regulation (EU) 2016/679.
The data controller shall ensure that the risk mitigation actions resulting from processing DPIAs are effectively implemented.

Consistent with a life cycle perspective, the organization shall maintain documented information to demonstrate the processes have been carried out as planned and demonstrate the compliance of products and/or services to their requirements (see 7.3).

Any event during processing operations which breaches the rights of data subject shall be recorded as a nonconformity and shall initiate a corrective action.

8.2 Control of subcontractors and service providers

The organization shall ensure that outsourced processes are controlled or influenced in accordance with articles 27 and 28 of Regulation (EU) 2016/679 and to ensure the protection of data subject's rights. The type and extent of control or influence to be applied shall be defined taking into account the nature, scope, context and purposes of the processing resulting in a high risk to the rights and freedoms of natural persons.

In particular:

- the organization shall only use suppliers providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the compliance obligations (see 5.2) and ensure the protection of the data subject's rights;
- processing by an external provider shall be governed by a contract that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the data controller.

That contract shall stipulate, in particular, that the external provider:

(a) processes the personal data only on documented instructions from the data controller, including with regard to transfers of personal data to a third country or an international organization;
(b) ensures that persons authorized to process the personal data have committed themselves to confidentiality;
(c) takes all specified measures related to personal data security;
(d) assists the data controller by appropriate technical and organizational measures adapted to the nature of processing;
(e) assists the data controller in ensuring compliance with the obligations pursuant to articles 32 to 36 taking into account the nature of processing;
(f) at the choice of the data controller, deletes or returns all the personal data to the organization after the end of the provision of services relating to processing;
(g) makes available to the organization all information necessary to demonstrate compliance with the compliance obligations and contribute to audits, including inspections, conducted by the organization or another auditor mandated by the organization;
(h) shall not engage another processor and/or service provider without prior specific or general written authorization of the data controller;
(i) shall notify the data controller without undue delay after becoming aware of a personal data breach and any infirgment to Regulation (EU) 2016/679.

A data controller or data processor may transfer personal data to a third country or an international organization only if the transfer is compliant with one of the provisions expressed in articles 27, 44, 45 and 46 of Regulation (EU) 2016/679.

9. Resources

The organization shall determine and provide resources needed for the implementation of technical and organizational measures to ensure compliance with personal data protection requirements.

9.1 Infrastructure

The organization shall implement technical and organizational measures which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing as appropriate considering the type and nature of processing and the outcomes of the Data Protection Impact Assessment.

In particular, such measures shall ensure that by default personal data are not made accessible to an indefinite number of natural persons without the individual's intervention.

Where proportionate in relation to processing activities, the measures referred to above shall include the implementation of appropriate data protection policies by the organization. These measures shall specify appropriate security controls along the different phases of data collection, storage, handling and transfer.

The organization shall implement procedures which ensure that access by personnel to personal information is restricted to the personnel who need to have such access.

The organization shall implement appropriate process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

NOTE: Where appropriate, the organization may consider compliance with ISO/IEC 27001.

NOTE: ISO/IEC 27002:2013 can be used as a guideline to identify the appropriate measures to be implemented.

NOTE: Particular attention should be paid to storage of personal data on portable devices or equipment.

9.2 Personnel

9.2.1 Competence

The organization shall:

a) determine the necessary competence of person(s) performing work that affects personal data protection and its ability to fulfil its compliance obligations including communication;
b) ensure that these person(s) are competent on the basis of appropriate education, training or experience;
c) determine training needs associated with the Data Protection Impact Assessments, as appropriate;
d) maintain the competences of its personnel involved in personal data protection considering changes in technologies and practices;
e) and where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken.

In particular, the person(s) in charge of the implementation of the "management system" within the organization shall have been trained on Regulation (EU) 2016/679.

Records of all trainings shall be available. This shall include as a minimum:

a) the name of the trainee and confirmation of attendance;
b) the date and duration of the training;
c) the title or course contents, as appropriate;
d) the training provider.

9.2.2 Awareness

The organization shall ensure that all relevant personnel are aware of:

a) the personal data protection policies and procedures;
b) the actual or potential personal data breaches associated with their work;
c) the implications of not conforming with the organization's personal data protection policy and its compliance obligations.

Appendix 1 - Introduction

0.1 General

The potential benefits to an organization of implementing a "management system" related to personal data protection based on this standard are:

a) the ability to consistently provide products and services that meet applicable statutory and regulatory requirements;
b) addressing risks and opportunities associated with its context and objectives;
c) the ability to demonstrate compliance with regulatory requirements.

This standard employs the process approach, which incorporates the Plan-Do-Check-Act (PDCA) cycle and risk-based thinking.

In particular it includes:

- the adoption of internal rules;
- the retention of records of any processing carried out under the responsibility of the controller or subcontractor, i.e. a description of each processing operation implemented;
- the implementation of an impact assessment for processings presenting particular risks with regard to the rights and freedoms of natural persons;
- respect for the principle of transparency in decisive transactions relating to the protection of personal data;
- the implementation of the "data protection by-design" and "data protection by-default" approaches in projects;
- the appointment of a data protection officer;
- documentation and recording of compliance actions.

0.2 Aim of this certification scheme

The purpose of this certification scheme is to provide organizations with a framework of technical and organizational measures and processes to comply with Regulation (EU) 2016/679 related to personal data protection and respond to technological advances.

A systematic approach to personal data protection management can provide top management with information to build success over the long term and create conditions to achieve compliance by:

- protecting personal data by preventing or mitigating personal data breaches;
- assisting the organization in the fulfilment of compliance obligations;
- controlling or influencing the way the organization's products and services are designed, developed, processed, and disposed by using a life cycle perspective that can prevent personal data protection breaches;
- communicating appropriate information to relevant interested parties.

0.3 Process approach

0.3.1 General

1 **Accountability principle.** This is a general principle of liability to the data controller for any processing of personal data which it carries out itself or which is carried out on its behalf.

2 Consequently, this obligation requires the controller to implement appropriate technical and organizational measures in order to carry out the processing in compliance with the requirements of the Regulation.

3 **Internal rules.** Therefore, in order to comply with this obligation, the data controller must describe in detail the necessary obligations to comply with the Regulation and provide evidence, in particular by adopting internal rules and mechanisms.

4 In addition, the controller must take a pro-active approach whereby it is able to demonstrate compliance without waiting for irregularities to be reported to it. It shall adopt internal rules and implement appropriate measures to ensure and be able to demonstrate that the processing of data is carried out in compliance with the Regulation.

5 The scope of these obligations takes into account:

- the purpose of the processing operations;
- the risks of infringing the rights and freedoms of natural persons.

6 Depending on the risks associated with the processing and the types of data being processed, the measures to be implemented range from documentation to the implementation of security obligations and the implementation of an impact assessment.

7 **Transparency.** The controller is subject to an obligation of transparency and traceability of documents in order to be able to be held accountable. It must at all times be able to identify and document the measures taken to comply with the requirements of the Regulation and be able to demonstrate that it has fulfilled its personal data protection obligations. All the actions of its data protection policy shall be documented in order to demonstrate its implementation to the supervisory authorities.

8 **Data protection by design.** The principle of "data protection by design" requires organizations to take into account the respect for data protection in the design of products, services and systems using personal data.

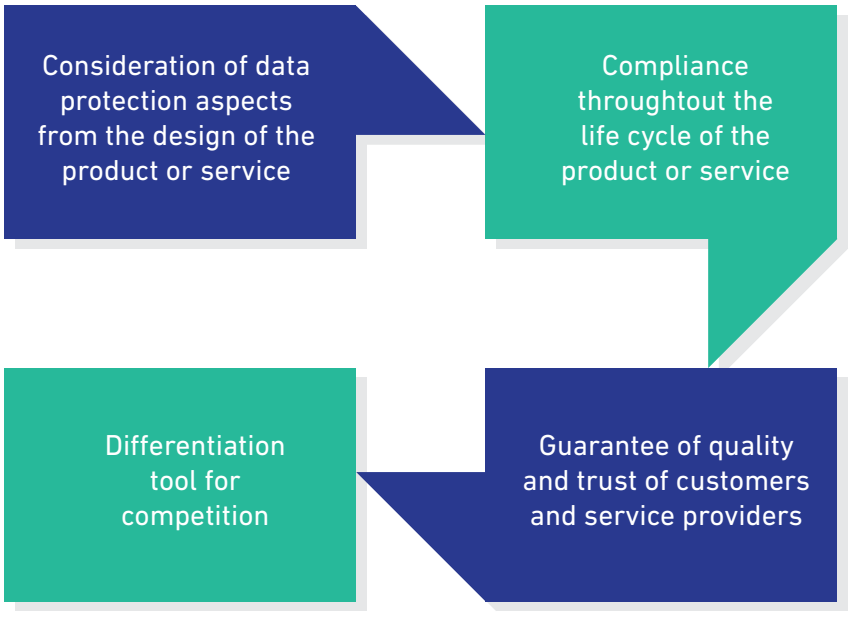

Figure 1: Data protection by design

9 **Data protection by default.** The «data protection by default» principle requires organizations to have an information system that guarantees a high level of data protection at all stages (registration, operation, administration, integrity and update). The security of the information system must be ensured in all its physical or logical elements. This rule implies that the security status of the information system must be monitored, in relation to the manufacturer's specifications, the vulnerable aspects and the updates.

The approach of the Regulation can be formalized as follows:

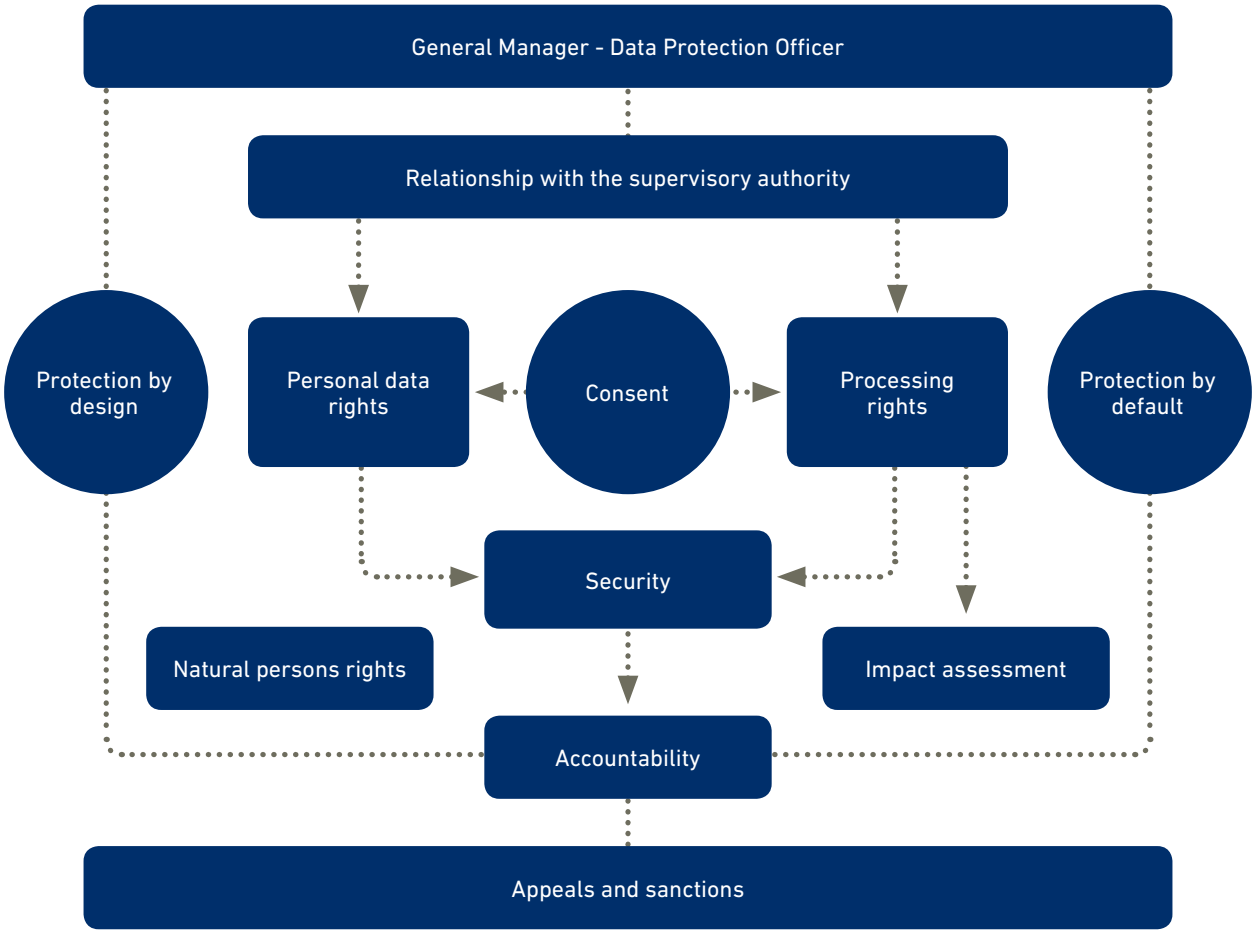

Figure 2: The legal approach of Regulation

Appendix 2 – Cross-reference matrix

Certification Scheme versus GDPR

Certification Scheme		REGULATION EU 2016/679
0	Foreword	Article 1 ; Article 2; Article 40; Article 42
1	Scope	Article 24 (3); Article 25(3); Article 28(5); Article 42
2	References	
3	Terms and definitions	
4	Organization and Structure	
4.1	Leadership and commitment	Article 24
4.2	Policy	
4.2.1	Establishing the personal data protection policy	
4.2.2	Communicating the personal data protection policy	
4.3	Organizational roles, responsibilities and authorities	Article 24 ; Article 28 ; Article 37; Article 38; Article 39
4.3.1	Organization and responsibilities	
4.3.2	Data Protection Officer	
5	Personal Data Risk Management	
5.1	General	Article 24 ; Article 28
5.2	Data Protection Impact Assessment	Article 35, Article 36
5.3	Compliance obligations	Article 6 ; Article 24 ; Article 28
5.4	Managing Personal Data Breaches	Article 33; Article 34
6	Management System	
6.1	Manual and procedures	Article 5
6.2	Documented information	Article 30 (register), article 35 (DPIA)
6.3	Performance evaluation	Article 24
6.4	Internal audit	Article 24
6.5	Nonconformity and corrective action	
6.6	Complaints	
6.7	Management review	Article 24
6.8	Communication	
6.8.1	General	
6.8.2	Internal communication	
6.8.3	External communication	Article 6; Article 7; Article 12; Article 13; Article 14; Article 15; Article 16; Article 17; Article 18; Article 19; Article 20; Article 21; Article 22; Article 23; Article 34
7	Product and/or service control	
7.1	Requirements for products and service	
7.2	Design and development of products and/or services	Article 5 ; Article 7 ; Article 12 to 23; Article 25; Article 32; Article 36
7.3	Release of products and/or services	Article 30
8	Operational control	
8.1	Processing control	Article 5; Article 24; Article 12 to 23 ; Article 32; Article 36
8.2	Control of subcontractors and service providers	Article 27 ; Article 28; Article 44 ; Article 45; Article 46
9	Resources	
9.1	Infrastructure	Article 24 (2); Article 25 (1) (2); Article 28 ; Article 32 1(d)
9.2	Personnel	
9.2.1	Competence	Article 24 ; Article 25 ; Article 37
9.2.2	Awareness	Article 32 (4)

Appendix 2 – Cross-reference matrix

GDPR versus Certification Scheme

Chapter	Section	Article		Certification Scheme
General provisions		Article 1	Subject-matter and objectives	Foreword Scope Appendix 1
		Article 2	Material scope	Appendix 1
		Article 3	Territorial scope	Foreword Scope 8.2 Control of subcontractors and service providers
		Article 4	Definitions	3 Terms and definitions
Principles		Article 5	Principles relating to processing of personal data	6.1 Manual and procedures 7.2 Design and development of products and/or services 8.1 Processing control
		Article 6	Lawfulness of processing	5.3 Compliance obligations 6.8.3 External communication + Appendix 1
		Article 7	Conditions for consent	6.8.3 External communication 7.2 Design and development of products and/or services
		Article 8	Conditions applicable to child's relation to Impact Assessment information society services	5.2 Data Protection consent in (Definitions 3.8 and 3.9)
		Article 9	Processing of special categories of personal data	
		Article 10	Processing of personal data relating to criminal convictions and offenses	
		Article 11	Processing which does not require identification	
Rights of the data subject	Transparency and modalities	Article 12	Transparent information, communication and modalities for the exercise of the rights of data subject	6.8.3 External communication 7.2 Design and development of products and/or services
	Information and access to personal data	Article 13	Information to be provided where personal data are collected from the data subject	6.8.3 External communication 7.2 Design and development of products and/or services 8.1 Processing control
		Article 14	Information to be provided where personal data have not been obtained from the data subject	6.8.3 External communication 7.2 Design and development of products and/or services 8.1 Processing control
		Article 15	Right of access by the data subject	6.8.3 External communication 6.2 Documented information 7.2 Design and development of products and/or services 8.1 Processing control

Appendix 2 – Cross-reference matrix

GDPR versus Certification Scheme

Chapter	Section	Article		Certification Scheme
		Article 16	Right to rectification	6.8.3 External communication 7.2 Design and development of products and/or services 8.1 Processing control
		Article 17	Right to erasure ('right to be forgotten')	6.8.3 External communication 7.2 Design and development of products and/or services 8.1 Processing control
	Rectification and erasure	Article 18	Right to restriction of processing	6.8.3 External communication 7.2 Design and development of products and/or services
		Article 19	Notification obligation regarding rectification or erasure of personal data or restriction	8.1 Processing control 6.8.3 External communication 7.2 Design and development of products and/or services 8.1 Processing control
		Article 20	Right to data portability	6.8.3 External communication 7.2 Design and development of products and/or services 8.1 Processing control
	Right to object and automated individual decision-making	Article 21	Right to object	6.8.3 External communication 7.2 Design and development of products and/or services
		Article 23	Restrictions	8.1 Processing control 6.8.3 External communication 7.2 Design and development of products and/or services
Controller and processor	General obligations	Article 24	Responsibility of the controller	8.1 Processing control Scope 4 Organization and Structure 4.1 Leadership and commitment 4.2 Policy 4.2.1 Establishing the personal data protection policy 4.2.2 Communicating the personal data protection policy 4.3 Organizational roles, responsibilities and authorities 4.3.1 Organization and responsibilities 4.3.2 Data Protection Officer

Appendix 2 – Cross-reference matrix

GDPR versus Certification Scheme

Chapter	Section	Article		Certification Scheme
Controller and processor	General obligations			5.1 General 5.3 Compliance obligations 6.3 Performance evaluation 6.4 Internal audit 6.7 Management review 8.1 Processing control 9.1 Infrastructure 9.2.1 Competence
		Article 25	Data protection by design and by default	7.2 Design and development of products and/or services 9.1 Infrastructure 9.2.1 Competence
		Article 26	Joint controllers	
		Article 27	Representatives of controllers or processors not established in the Union	8.2 Control of subcontractors and service providers
		Article 28	Processor	Scope 4.3 Organizational roles, responsibilities and authorities 4.3.1 Organization and responsibilities 4.3.2 Data Protection Officer 5.1 General 5.3 Compliance obligations 8.2 Control of subcontractors and service providers 9.1 Infrastructure
		Article 29	Processing under the authority of the controller or processor	
		Article 30	Records of processing activities	6.2 Documented information 7.3 Release of products and/or services
		Article 31	Cooperation with the supervisory authority	5.3 Compliance obligations
	Security of personal data	Article 32	Security of processing	7.2 Design and development of products and/or services 8.1 Processing control 9.1 Infrastructure 9.2.2 Awareness
		Article 33	Notification of a personal data breach to the supervisory authority	5.5 Managing Personal Data Breaches
		Article 34	Communication of a personal data breach to the data subject	5.1 Personal Data Risk Management / General 5.5 Managing Personal Data Breaches 6.8.3 External communication

Appendix 2 – Cross-reference matrix

GDPR versus Certification Scheme

Chapter	Section	Article		Certification Scheme
	Data protection impact assessment and prior consultation	Article 35	Data protection impact assessment	5.2 Data Protection Impact Assessment 6.2 Documented information 8.1 Processing control
		Article 36	Prior consultation	4.3.2 Data Protection Officer 5.2 Data Protection Impact Assessment 7.2 Design and development of products and/or services 8.1 Processing control
	Data protection officer	Article 37	Designation of the data protection officer	4.3 Organizational roles, responsibilities and authorities 4.3.1 Organization and responsibilities 4.3.2 Data Protection Officer 9.2.1 Competence
		Article 38	Position of the data protection officer	4.3 Organizational roles, responsibilities and authorities 4.3.1 Organization and responsibilities 4.3.2 Data Protection Officer
		Article 39	Tasks of the data protection officer	4.3 Organizational roles, responsibilities and authorities 4.3.1 Organization and responsibilities 4.3.2 Data Protection Officer
	Codes of conduct and certification	Article 40	Codes of conduct	Foreword
		Article 41	Monitoring of approved codes of conduct	Foreword 1; 7.2; 6.8.2; 7.1.1
		Article 42	Certification	Foreword Scope
		Article 43	Certification bodies	
Transfers of personal data to third countries or international organizations		Article 44	General principle for transfers	8.2 Control of subcontractors and service providers
		Article 45	Transfers on the basis of an adequacy decision	8.2 Control of subcontractors and service providers
		Article 46	Transfers subject to appropriate safeguards	8.2 Control of subcontractors and service providers
		Article 47	Binding corporate rules	6.8.2 / 7.1.1 / 7.2 + 3 Terms and definitions
		Article 48	Transfers or disclosures not authorized by Union law	
		Article 49	Derogations for specific situations	
		Article 50	International cooperation for the protection of personal data	

Appendix 3 – Applicability for data processor

	Certification Scheme	Processor applicability*
0	Foreword	
1	Scope	X
2	References	X
3	Terms and definitions	X
4	Organization ans Structure	X
4.1	Leadership and commitment	X
4.2	Policy	X
4.2.1	Establishing the personal data protection policy	X
4.2.2	Communicating the personal data protection policy	X
4.3	Organizational roles, responsibilities and authorities	X
4.3.1	Organization and responsabilities	X
4.3.2	Data Protection Officer	X
5	Personal Data Risk Management	
5.1	General	Partially applicable - Assist the data controller (b- DPIA outcomes)
5.2	Data Protection Impact Assessment	Assist the data controller
5.3	Compliance obligations	X
5.4	Managing Personal Data Breaches	Fully applicable. Liaise with the data controller regarding the notification/communication.
6	Management System	
6.1	Manual and procedures	X
6.2	Documented information	X
6.3	Performance evaluation	X
6.4	Internal audit	X
6.5	Nonconformity and corrective action	X
6.6	Complaints	X
6.7	Management review	Liaise with the data controller regarding the effectiveness of actions to address the DPIA
6.8	Communication	X
6.8.1	General	X
6.8.2	Internal communication	X
6.8.3	External communication	Partially applicable - Assist the data controller (paragraph 2)
7	Product and/or service control	
7.1	Requirements for products and service	X
7.2	Design and development of products and/or services	Assist the data controller
7.3	Release of products and/or services	Specific requirements for the register
8	Operational control	X
8.1	Processing control	Partially applicable. Assist the data controller
8.2	Control of subcontractors and service providers	Applicable: contract
9	Resources	
9.1	Infrastructure	Fully applicable. Liaise with the data controller regarding the outcomes of the DPIA
9.2	Personnel	Fully applicable. Liaise with the data controller regarding the DPIA
9.2.1	Competence	X
9.2.2	Awareness	X

*X = Fully applicable

ABOUT BUREAU VERITAS

Bureau Veritas is a world leader in testing, inspection, and certification. We help clients across all industries address challenges in quality, health & safety, environmental protection, enterprise risk and social responsibility. We support them in increasing performance throughout the life of their assets and products and via continuous improvement in their processes and management systems. Our teams worldwide are driven by strong purpose: to preserve people, assets and environment by identifying, preventing, managing and reducing risks.

BUREAU VERITAS CERTIFICATION HOLDING
Le Triangle de l'Arche - 8, Cours du Triangle, CS 90096
92937 Paris La Defense CEDEX
France