# GDPR-CERTIFIED ASSURANCE REPORT BASED PROCESSING ACTIVITIES

# CERTIFICATION CRITERIA

Working draft for public consultation - 29 May 2018


## Abstract

Document to the attention of organizations that want to obtain certification of processing activities under the GDPR-CARPA certification mechanism.



Commission Nationale pour la Protection des Données

alain.herrmann@cnpd.lu

This document was prepared by the Commission Nationale Pour la Protection des Données ('CNPD') in collaboration with representatives from the audit profession. It contains the criteria for the "GDPR-CARPA" certification mechanism. This document should be read in conjunction with the "GDPR-CARPA" certification mechanism document.

These certification criteria are a mandatory requirement to evaluate and report on controls over organizational and technical data protection measures, to be eligible for certification. Evaluation and reporting needs to follow the ISAE 3000 standard. Certification can only be granted by certification bodies that have been accredited by CNPD.

The "GDPR-CARPA" certification criteria might be subject to further changes after a period of public consultation, to best ensure verifiability, significance and suitability in regards to demonstrate compliance with GDPR and meet market demand.

About CNPD:

The National Commission for Data Protection (Commission Nationale pour la Protection des Données – CNPD) is an independent authority created by the Act of 2 August 2002 on the protection of individuals with regard to the processing of personal data. It verifies the lawfulness of the processing of personal data and ensures the respect of personal freedoms and fundamental rights with regard to data protection and privacy. Its mission also extends to ensuring the respect of the amended Act of 30 May 2005 regarding the specific rules for the protection of privacy in the sector of electronic communications. Under draft bill 7184, CNPD will be the independent public authority responsible for monitoring the application of GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

About ISAE 3000:

This International Standard on Assurance Engagements (ISAE) deals with assurance engagements other than audits or reviews of historical financial information. Assurance engagements include direct engagements, in which the practitioner measures or evaluates the underlying subject matter against a set of criteria. International Standard on Assurance Engagements (ISAE) 3000 (Revised), Assurance Engagements other than Audits or Reviews of Historical Financial Information, should be read in conjunction with the Preface to the International Standards on Quality Control, Auditing, Review, Other Assurance and Related Services Pronouncements.

Versioning:

| Version | Description | Date | Author |
|---|---|---|---|
| V0.1 | Initial version for public consultation | 29/05/2018 | CNPD |
| | | | |
| | | | |
| | | | |

## CONTENTS

# INTRODUCTION

The European Union General Data Protection Regulation (Regulation 2016/279) ('the GDPR'), which came into full effect on 25 May 2018, provides a modernised, accountable and fundamental rights compliance framework for data protection in Europe. A range of principles that facilitate compliance with the provisions of the GDPR are central to this new framework. These include mandatory requirements in specific circumstances (including the appointment of Data Protection Officers and carrying out data protection impact assessments) and voluntary measures such as codes of conduct and certification mechanisms.

Article 42(1) of the GDPR states that: "The Member States, the supervisory authorities, the [European Data Protection] Board and the European Commission shall encourage, in particular at the Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account".

Certifications are a virtuous business practices that can greatly improve transparency and accountability for data subjects, but also in business-to-business relations, for example between controllers and processors which are often seen as customers and providers. Recital 100 of the GDPR states that the establishment of certification mechanisms can enhance transparency and compliance with the Regulation and allow data subjects to assess the level of data protection of relevant products and services.

Certification under GDPR is a voluntary process to assist controllers and/or processors in demonstrating compliance to the GDPR to a supervisory authority or the data subjects.

Article 42(4) of GDPR clarifies that certification "does not reduce the responsibility of the controller or the processor for compliance" and therefore "is without prejudice to the tasks and powers of the supervisory authorities which are competent". It is however contributing to enhance trust between data protection authorities and other entities where certification bodies play a major role.

# DEFINITIONS

## GDPR (ARTICLE 4)

- '**Processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- '**Personal data'** means 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;
- **'GDPR'** refers to Regulation (EU) 2016/679 of the European parliament and 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);
- '**Controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the 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;
- '**Processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

## ISAE 3000 (A12)

- '**Assurance engagement**' means an engagement in which a practitioner aims to obtain sufficient appropriate evidence in order to express a conclusion designed to enhance the degree of confidence of intended users other than the responsible party about the subject matter information (that is, the outcome of the measurement or evaluation of an underlying subject matter against criteria). In the context of the GDPR-CARPA certification mechanism this term refers to the assurance report that underpins the certification decision.
- '**Criteria**" means the benchmarks used to measure or evaluate the underlying subject matter. The " applicable criteria" are the criteria used for the particular engagement. In the context of the GDPR-CARPA certification mechanism, this term refers to the criteria that are listed in this document.
- '**Practitioner**' means the individual(s) conducting the engagement (usually the engagement responsible or other members of the engagement team, or, as applicable, the firm). Where this ISAE expressly intends that a requirement or responsibility be fulfilled by the engagement partner, the term "engagement partner" rather than "practitioner" is used. In the context of the GDPR-CARPA certification mechanism this term refers to the staff/personnel employed or occupied by the accredited certification body that executes the certification assurance engagement field work.
- '**Engaging party'** means the part(ies) that engage the practitioner to perform the assurance engagement. In the context of the GDPR-CARPA certification mechanism those terms refers to either the data controller or the data processor who intends to obtain certification.

## ORGANISATION OF THE CRITERIA

The GDPR sets the ground for the development of certification criteria. Whereas fundamental requirements concerning the procedure of certification are addressed in Articles 42, 43 while also providing essential criteria for certification procedures, the basis for certification criteria must be derived from the principles and rules set by the GDPR and help to provide assurance that principles and rules are fulfilled.

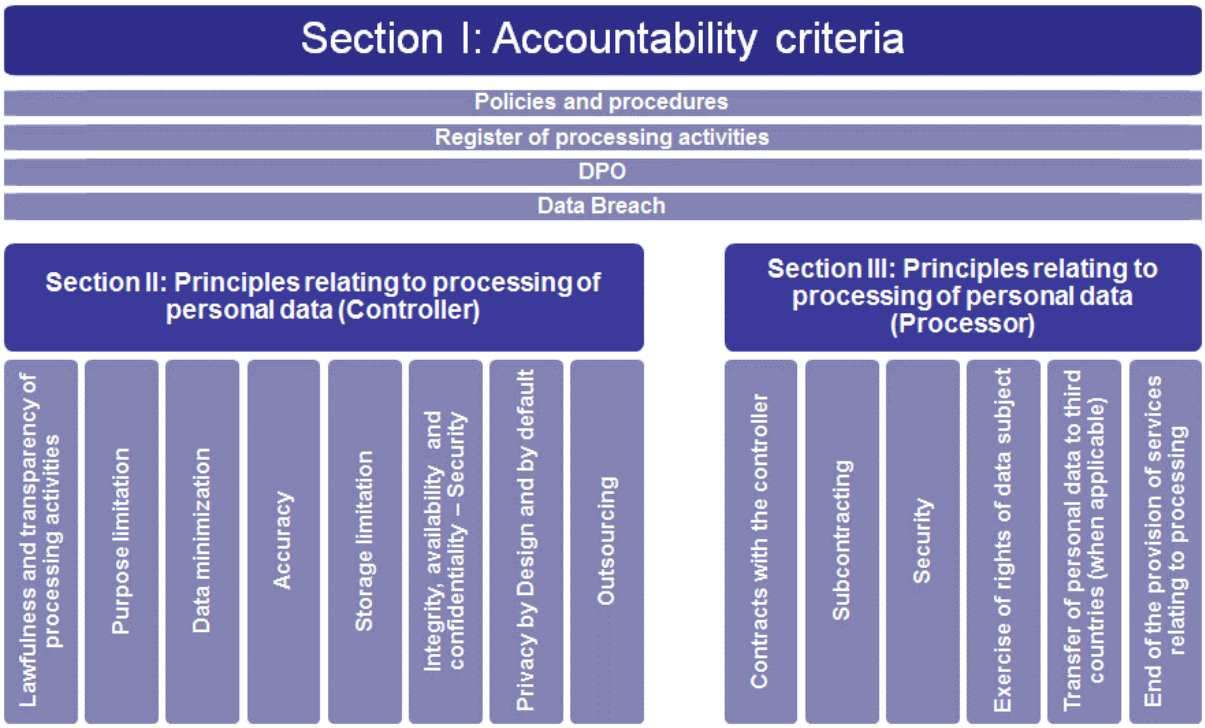
The criteria of a certification mechanism shall be applicable to individual certification engagements. They should be able to cover all relevant aspects of data processing and, where necessary, also take into account the purposes of processing.

Depending on the area (e.g. health sector) and scope of certification (multiple or single processing operations) certification criteria shall always address, inter alia, the following compliance aspects in support of the assessment of the processing operation:

- the legitimacy of data processing pursuant to Article 6,
- the principles of data processing pursuant to Article 5,
- the data subjects' rights pursuant to Articles 12-23,
- the obligation to notify data breaches pursuant to article 33,
- data protection by design and by default, pursuant to article 25,
- that a data protection impact assessment, pursuant to article 35(7)(d) has been conducted, if applicable,
- technical and organisational measures put in place pursuant to Articles 32.

Taking the above into account the GDPR-CARPA certification criteria have been aligned to the "Principles relating to processing of personal data" as defined under article 5 of GDPR, and complemented by the other requirements as set out above.

The criteria are organized according to the sections as dfollows:



## SECTION I: ACCOUNTABILITY CRITERIA

This section contains the criteria relevant to how an entity manages personal data protection concerns from a governance point of view to ensure its management can assume accountability. Criteria within this section contain a flag that indicates if they apply to entities that request certification as data controller or as data processor – if entities act as controller or as processor for at least one processing activity within the scope of the certification, they need to comply with all of the requirements set out in this section.

## SECTION II: PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA (CONTROLLER)

This section contains the criteria relevant to how an entity manages personal data protection requirements for a given processing activity in scope, where it acts as controller. This section is composed of sub-sections, which respectively relate to the principles of processing of personal data as defined under GDPR, and complemented by additional relevant elements, namely:

- Subsection II-a: Lawfulness, fairness and transparency
- Subsection II-b: Purpose limitation
- Subsection II-c: Data minimization
- Subsection II-d: Accuracy
- Subsection II-e: Storage limitation
- Subsection II-f: Integrity and confidentiality - Security
- Subsection II-g: Privacy by design and by default
- Subsection II-h: Outsourcing

## SECTION III: PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA (PROCESSOR)

This section contains the criteria relevant to how an entity manages personal data protection requirements for a given data processing activity in scope, where it acts as data processor.

## MAPPING OF GDPR-CARPA CERTIFICATION CRITERIA

The below mapping table serves as a reference table to demonstrate GDPR-CARPA Certification Criteria meet the mandatory compliance aspects.

| Mandatory compliance aspects | GDPR-CARPA Criteria |
|---|---|
| | Section I - Accountability |
| **Legitimacy of data processing pursuant to Article 6,** | Section II - Lawfulness - Processing based on legitimate interest |
| **Principles of data processing pursuant to Article 5,** | Section II - Lawfulness<br>Section II - Transparency |
| **Data subjects' rights pursuant to Articles 12-23,** | Section I – Data Subject Rights<br>Section II – Accuracy<br>Section III – Exercise of rights of data subject |
| **Obligation to notify data breaches pursuant to article 33,** | Section I – Policies and procedures<br>Section I – Data breach |
| **Data protection by design and by default, pursuant to article 25,** | Section II – Privacy by design and by default |
| **Data protection impact assessment, pursuant to article 35(7)(d) has been conducted, if applicable,** | Section I – DPO – Competences<br>Section I – DPO - Tasks |
| **Technical and organisational measures put in place pursuant to Articles 32.** | Section II – Integrity and confidentiality – Security<br>Section III - Security |

## APPLICATION OF CRITERIA

The criteria for the GDPR-CARPA certification mechanism are met only if all the criteria are addressed by the engagement. For sections II and III, all criteria need to be met for each processing activity in scope – either in the role of data controller or processor.

The practitioner must report on all of the GDPR-CARPA certification criteria. However, in limited circumstances, such as when the scope of the engagement is to report on a particular criterion that is not relevant to the processing activity by the entity, one or more criteria may not be applicable to the engagement. In such situations, the one or more criteria would not need to be addressed. Every exclusion of a criteria must be documented within the assurance report with the reasoning for doing so.

Further, the common criteria (Section I) must be applied regardless of which processing activities are included within the scope of the engagement.

For the ISAE 3000 report based on the GDPR-CARPA certification criteria to qualify for a certification it must be a type 2 report. Type 1 reports might be used in a transition phase, as it is common practice, but they cannot effectively support a certificate. A type 2 engagement provides assurance over (1) the fairness of the presentation of the description of the entity's system; and (2) the suitability of design, implementation and operating effectiveness of the controls throughout a period. A type 1 engagement provides assurance over (1) the fairness of the presentation of the description of the service entity's system; and the suitability of design and implementation of the controls as at a date. A type 1 engagement does not provide assurance over the operating effectiveness of the controls throughout a period, as a type 2 engagement would.

The ISAE 3000 report on which is based a certificate must provide "Reasonable assurance" (i.e. not "limited assurance").

According to the attestation standards, the criteria used in an attestation engagement shall be suitable and available to report users. Attributes of suitable criteria are as follows:

- Relevance: Relevant criteria result in subject matter information that assists decision-making by the intended users.
- Completeness: Criteria are complete when subject matter information prepared in accordance with them does not omit relevant factors that could reasonably be expected to affect decisions of the intended users made on the basis of that subject matter information. Complete criteria include, where relevant, benchmarks for presentation and disclosure.
- Reliability: Reliable criteria allow reasonably consistent measurement or evaluation of the underlying subject matter including, where relevant, presentation and disclosure, when used in similar circumstances by different practitioners.
- Neutrality: Neutral criteria result in subject matter information that is free from bias as appropriate in the engagement circumstances.
- Understandability: Understandable criteria result in subject matter information that can be understood by the intended users.

In addition to being suitable, ISAE 3000 indicates that the criteria used in an attestation engagement must be available to intend users as defined by the engaging party. The publication of the GDPR-CARPA certification criteria by CNPD makes the criteria publicly available.

## SCOPE OF THE CERTIFICATION

GDPR provides a broad scope for what can be certified (also known as "the object of certification" or "Target of Evaluation" (ToE)), as long as the focus is on demonstrating compliance with GDPR of processing operations by controllers and processors" (Article 42.1).

The "object of certification" under the GDPR-CARPA certification mechanism is a set of "processing activities" as defined under GDPR. It is up to the entity to be certified to define the processing activities in scope – this approach adds flexibility to the mechanism. Entities can start with a limited scope and extend it over the years, they can focus on key processing activities – or those that are most relevant in regards to demonstrating compliance. An entity can select processing activities for which it acts as controller or as a processor. The description on which sections apply to which processing activity is further described under sections "ORGANISATION OF THE CRITERIA" and "APPLICATION OF CRITERIA".

As the certification decision relies upon the ISAE 3000 attestation report, it is clear that the scope of the attestation assurance must cover at least all processing activities that are in scope of the certification.

The concept of processing is specified in Article 4 (2) in the GDPR. It shall cover all the relevant components of a processing in such a way as to make them available for assessment for the purpose of certification, which is to demonstrate compliance with the GDPR. In order to fully understand processing operations, it has proved useful to distinguish at least four different levels of significant influencing factors or components for the evaluation of processing operations. The first level is directed to the organisation of the controller or processor, e.g. a private or public organisation and its specific legal ecosystem. The second level addresses the organisational circumstances and the purpose or purposes for which the processing operation is performed, e.g. the department and the people in charge of the operation. On a third level, the functional application is assessed which has to implement the purpose. And finally, the fourth level, considers the entire IT respectively IT infrastructure and the functions provided. This level includes operating systems, virtual systems, databases, authentication and authorization systems, routers and firewalls, storage systems such as SAN or NAS, an organization's communication infrastructure or Internet access, as well as the technical measures which must be implemented.

The following table is an illustrative example of how the certification scope for a given entity is defined:

| Processing activity (as per the register) | Role | Level 1 Organisation | Level 2 Circumstances / purpose | Level 3 functional application | Level 4 IT infrastructure |
|---|---|---|---|---|---|
| **Recruitment** | Controller | Financial institution | HR department | SAP-HR | Windows server farm, Oracle DB |
| **Newsletter** | Controller | Financial institution | Marketing | CRM | Cloud solution-SAAS |
| **AML/KYC** | Controller | Financial institution | Compliance<br>Client relationship Managers | World Check<br>Avaloq | Cloud solution-SAAS<br>Unix servers – Oracle DB |

# GDPR-CARPA CERTIFICATION CRITERIA

## SECTION I: ACCOUNTABILITY CRITERIA / GOVERNANCE CRITERIA

| Ref. | Label | Description | Controller | Processor |
|---|---|---|---|---|
| | | **Policies and procedures** | | |
| **I-1** | Accountability<br>(GDPR Article 24)<br>(Recitals 74, 75, 76, 77, 84) | The entity has implemented organizational measures that ensure authorized management is **informed, involved and accountable of personal data processing activities**.<br>Measures include, but are not limited to:<br>• the implementation of appropriate data protection policies;<br>• formal allocation of roles and responsibilities;<br>• formal reporting lines;<br>• documentation of decisions impacting data protection. | X | X |
| **I-2** | Review of policies and procedures<br>(GDPR Article 24)<br>(Recitals 74, 75, 76, 77, 84) | The entity reviews, on a regular basis and at least annually, **the operational effectiveness of its data protection governance policies and procedures** and adapts them accordingly.<br>Policies should cover at least the following topics:<br>• the record of processing activities;<br>• data subject's right;<br>• the DPO's roles and responsibilities (if applicable);<br>• data breach handling;<br>• data protection principles;<br>• data transfers (if applicable);<br>• use of processors (if applicable).<br>The review is:<br>• performed or delegated by authorized management to resources with relevant business, legal and technical competencies;<br>• documented and exceptions are followed up upon;<br>• approved by the entities management. | X | X |

| Ref. | Label | Description | Controller | Processor |
|---|---|---|---|---|
| | | Point of focus: The policies and procedures in relation to the record of processing activities should cover the requirements listed in sections I-3 to I-5. | | |
| | | **Register of processing activities** | | |
| I-3 | Management of the record<br>(GDPR Article 30)<br>(Recital 82) | The entity's management **reviews and approves** on a regular basis and at least annually, or when significant changes in the data privacy landscape of the entity occur, **the record of the personal data processing activities under its responsibility** to **ensure completeness and accuracy of the record**.<br>The review is :<br>• performed by resources with relevant business, legal and technical competencies;<br>• documented and exceptions are followed up upon;<br>• approved by the entities management. | X | |
| I-4 | Management of the record<br>(GDPR Article 30)<br>(Recital 82) | The entity's management **reviews and approves** on a regular basis and at least annually **the record** of all categories of processing activities carried out on behalf of a controller to **ensure completeness and accuracy of the record**.<br>The review is :<br>• performed by resources with relevant business, legal and technical competencies;<br>• documented and exceptions are followed up upon;<br>• approved by the entities management. | | X |
| I-5 | Content<br>(GDPR Article 30)<br>(Recital 82) | The entity has implemented a **record of personal data processing activities that contains, at least, and for each processing activity**:<br>• the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;<br>• the purposes of the processing;<br>• a description of the categories of data subjects and of the categories of personal data;<br>• the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations;<br>• transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in absence of an EU Commission adequacy decision, the documentation of suitable safeguards;<br>• the envisaged time limits for erasure of the different categories of data;<br>• a general description of the technical and organizational security measures to ensure a level of security appropriate to the risk of the processing. | X | |

| Ref. | Label | Description | Controller | Processor |
|---|---|---|---|---|
| I-6 | Content<br>(GDPR Article 30)<br>(Recital 82) | The entity has implemented a **record** of all categories of processing activities carried out on behalf of a controller **that contains, at least, and for each category of processing activity**:<br>• the name and contact details of the subprocessor(s) and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;<br>• the categories of processing carried out on behalf of each controller;<br>• where possible, a general description of the technical and organisational security measures to ensure a level of security appropriate to the risk of the processing.<br>• 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, in the case of transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in absence of an EU Commission adequacy decision, the documentation of suitable safeguards; | | X |
| | | **Data Subject Rights** | | |
| I-7 | Data subjects rights<br>(GDPR Article 12)<br>(Recitals 58, 61) | The entity has implemented measures to ensure that:<br>• **a contact point has been appointed** for receiving data subject's request for exercising their rights, that is easily reachable;<br>• **requests are recorded** and their timely conducted execution documented;<br>• for rejected requests, the **justification of the reject is documented** and communicated to the data subject (or the controller). | X | X |
| | | **DPO** | | |
| I-8 | Designation<br>(GDPR Article 37)<br>(Recital 97) | The entity has assessed and **documented requirement to designate a DPO**.<br>In case the entity decides:<br>• not to designate a DPO, **the decision together with the assessments that leads to the decision is approved** by the entities management;<br>• to designate a DPO, the entities management has **formally designated the DPO** at the applicable supervisory authority. | X | X |
| I-9 | Competencies<br>(GDPR Article 37)<br>(Recital 97) | The entity that has decided to designate a DPO has assessed **his/her professional qualities** and in particular:<br>• his/her **expert knowledge of data protection law and practices;**<br>• His/her **ability to fulfil the tasks mentioned in I-11**; | X | X |

| Ref. | Label | Description | Controller | Processor |
|---|---|---|---|---|
| I-10 | Position<br>(GDPR Article 38)<br>(Recital 97) | The entity that has decided to designate a DPO has implemented measures that:<br>• **ensure that the DPO is involved**, properly and in a timely manner, in all issues which relate to the protection of personal data;<br>• ensure that **the DPO is supported** by the entities management in performing his/her tasks, in particular by providing time and resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his/her or her expert knowledge;<br>• ensure that the **DPO does not receive any instructions** regarding the exercise of his/her tasks. He or she shall not be dismissed or penalised for performing his/her tasks. The data protection officer shall directly report to the highest management level of the controller or the processor;<br>• ensure that **data subjects can contact the DPO** with regard to all issues related to processing of their personal data and to the exercise of their rights under GDPR;<br>• ensure that the **DPO is bound by secrecy or confidentiality** concerning the performance of his/her tasks, in accordance with Union or Member State law;<br>• ensure that the **DPO is not involved in tasks and duties that could result in a conflict of interests**. | X | X |
| I-11 | Tasks<br>(GDPR Article 39) | The entity that has decided to designate a DPO has mandated him/her to execute, at least the following tasks:<br>• **inform and advise the entity** and its employees who carry out processing activities, of their obligations pursuant to GDPR and to other Union or Member State data protection provisions;<br>• **Monitor and report towards management on compliance with GDPR**, with other Union or Member State data protection provisions and with the policies of the entity in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;<br>• **provide advice** where requested as regards the data protection impact assessment and monitor its performance;<br>• **cooperate with the supervisory authority**;<br>• **act as the contact point for the supervisory authority** on issues relating to processing, including the prior consultation for DPIAs, and to consult, where appropriate, with regard to any other matter.<br>Point of focus: Requirements of the data protection officer shall be assessed in regards of the latest version of the "Guidelines on Data Protection Officers ('DPO'), wp243" from the data protection authorities article 29 working party. | X | X |

| Data breach | | | | |
|---|---|---|---|---|
| I-12 | Data breach<br>(GDPR Articles 33-34)<br>(Recitals 85, 86, 87, 88) | The entity has implemented technical and/or organizational measures to **effectively detect, manage and if applicable notify personal data breaches**. The measures must cover at least:<br>• the **setup and management of a record of personal data breaches**. The record of personal data breaches must contain at least, for each data breach: a description of the event, the impact of the event including the risk analysis for data subjects, the root cause, the remediation action taken and the evidence of notification.<br>• the **systematic assessment of the potential risk** to the rights and freedoms of natural persons caused by a data breach;<br>• the **ability to communicate with data subjects / data controller(s)**, if required or decided upon on a voluntary basis. This communication shall contain at least: a description of the nature of the personal data breach; the name and contact details of the data protection officer or other contact point where more information can be obtained; a description of the likely consequences of the personal data breach; a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects; this message must be individual and dedicated only to this breach.<br>Point of focus: The requirements requested for this section "Data breach" shall be assessed in regards of the latest version of the "Guidelines on personal data breach notification under regulation 2016/679 – WP250" from the data protection authorities article 29 working party. | X | |
| I-13 | Notification towards the controller<br>(GDPR Article 33)<br>(Recitals 85, 86, 87, 88) | The entity has implemented technical and/or organizational measures to **effectively detect, manage and if applicable notify personal data breaches towards the controller(s) without undue delay after becoming aware of a personal data breach.** The notification referred shall at least:<br>• describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;<br>• communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;<br>• describe the likely consequences of the personal data breach, if possible;<br>• describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.<br>Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.<br>Point of focus: The requirements requested for this section "Data breach" shall be assessed in regards of the latest version of the "Guidelines on personal data breach notification under regulation 2016/679 – WP250" from the data protection authorities article 29 working party. | | X |

## SECTION II: PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA (CONTROLLER)

### SUBSECTION II- A: LAWFULNESS AND TRANSPARENCY OF PROCESSING ACTIVITIES

| Ref. | Label | Description |
|---|---|---|
| | | **Lawfulness** |
| **II-a-1** | Identification of a valid legal basis<br>(GDPR Article 6)<br>(Recitals 135, 136, 137, 138) | The entity has implemented measures to ensure that **a valid legal basis is identified** for each processing activity.<br>The assessment of the validity of the identified legal basis is documented and, **involved relevant stakeholders**. |
| **II-a-2** | Processing based on consent<br>(GDPR Article 4, 7)<br>(Recitals 32, 42, 43, from 101 to 116) | For each processing activity in scope, where processing is based on the data subjects consent, the entity has implemented measures to ensure:<br>• consent is **collected and stored in an unaltered manner**;<br>• **consent** has been obtained in a formal way;<br>• processing is stopped in case a **data subject withdraws his consent**. |
| **II-a-3** | Processing based on contract<br>(GDPR Article 6)<br>(Recitals 135, 136, 137, 138) | For each processing activity in scope, where 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, the entity has implemented measures to ensure:<br>• contracts are **collected and stored in a unaltered manner;**<br>• **relevant data protection sections** of the contract have been formally integrated and exceptions escalated. |
| **II-a-4** | Processing based on legal obligation<br>(GDPR Article 6)<br>(Recitals 135, 136, 137, 138) | For each processing activity in scope, where processing is necessary for compliance with a legal obligation to which the entity is subject, the entity has:<br>• **identified the legal obligation and formally assessed its application**.<br>• requested the **formal opinion of its DPO** – if it designated a DPO, or by management in case no DPO has been designated. |
| **II-a-5** | Processing based on vital interest<br>(GDPR Article 6)<br>(Recitals 135, 136, 137, 138) | For each processing activity in scope, where processing is necessary in order to protect the vital interests of the data subject or of another natural person, the entity has:<br>• formally **assessed the presence of the vital interest at the moment the processing** takes place.<br>• requested the **formal opinion of its DPO** – if it designated a DPO, or by management in case no DPO has been designated. |

| | | |
|---|---|---|
| **II-a-6** | Processing based on public interest<br>(GDPR Article 6)<br>(Recitals 135, 136, 137, 138) | For each processing activity in scope, where 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 entity, the entity has:<br>• obtained from the relevant public authority a **formal mandate to execute** the processing activity;<br>• implemented **measure to suspend the processing activity** in case a data subject executes his right of opposition. |
| **II-a-7** | Processing based on legitimate interest<br>(GDPR Article 6)<br>(Recitals 135, 136, 137, 138) | For each processing activity in scope, where processing is necessary for the purposes of the legitimate interests pursued by the entity or by a third party, the entity has:<br>• assessed if legitimate interest as a legal basis is **legally applicable for the entity;**<br>• formally **assessed that the entity's interests are not overridden** by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child;<br>• implemented appropriate measures to ensure that **data subject's interests have been expressed and taken into consideration** during the assessment;<br>• requested the **formal opinion of its DPO** – if it designated a DPO, or by management in case no DPO has been designated.<br>• formal **approval from its management** on the assessment;<br>• implemented measure to **suspend the processing** in case a data subject has executed his right of opposition. |
| **II-a-8** | Processing of special categories of personal data<br>(GDPR Article 9)<br>(Recitals 33, 35, 51, 52, 53, 54, 55, 75) | For each processing activity in scope, the entity has implemented measures that ensure that processing of **special categories of data is strictly prohibited unless a valid legal basis as required in the GDPR is identified**. If such a case the entity has:<br>• requested the formal opinion of its DPO – if it designated a DPO, or by management in case no DPO has been designated;<br>• formal approval from its management on the assessment. |
| **II-a-9** | Right to object<br>(GDPR Article 21)<br>(Recitals 65, 70 73) | For each processing activity in scope, the entity has implemented measures that ensure that it can **effectively implement the "right to object"** of a data subject. |
| **Transparency** | | |
| **II-a-10** | Availability of information (direct collection)<br>(GDPR Article 13)<br>(Recitals 39, 58, 59, 60, 61, 62, 63) | For each processing activity in scope, where personal data are collected from the data subject, the entity has implemented measures to **ensure that the data subject is provided with the following information** at the time when personal data is obtained/collected:<br>• the **identity and the contact details of the entity** and, where applicable, of the entity's representative; or the **contact details of the DPO**, if a DPO has been designated;<br>• the **purposes of the processing** for which the personal data are intended as well as the legal basis for the processing;<br>• where the processing is based on the legitimate interest of the entity, **the legitimate interests pursued** by the entity or by a third party; |

| | | |
|---|---|---|
| | | • **the recipients or categories of recipients** of the personal data, if any;<br>• where applicable, the fact that the **entity intends to transfer personal data to a third country** or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;<br>• **the period for which the personal data will be stored**, or if that is not possible, the criteria used to determine that period;<br>• the existence of the right to request from the entity **access to and rectification or erasure of personal data** or **restriction of processing** concerning the data subject or to **object to processing** as well as the **right to data portability**;<br>• where the processing is based on point data subjects consent, **the existence of the right to withdraw consent** at any time, without affecting the lawfulness of processing based on consent before its withdrawal;<br>• the **right to lodge a complaint** with a supervisory authority;<br>• whether the provision of personal data is a statutory or contractual requirement, or a **requirement necessary to enter into a contract**, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;<br>• **the existence of automated decision-making, including profiling**, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.<br><br>The entity has **documented the relevant exception that might apply** for each information not provided by the entity to the data subject. (Art- 13-4) |
| **II-a-11** | Availability of information (indirect collection)<br><br>(GDPR Article 11, 14)<br><br>(Recital 57) | For each processing activity in scope, where personal data have not been obtained from the data subject, the entity has implemented measures to **ensure that the data subject is provided with the following information within a reasonable period** after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed.<br><br>• **the identity and the contact details of the entity** and, where applicable, of the entity's representative;<br>• **the contact details of the DPO**, if a DPO has been designated;<br>• **the purposes of the processing** for which the personal data are intended as well as the legal basis for the processing;<br>• **the categories of personal data** concerned;<br>• **the recipients or categories of recipients** of the personal data, if any;<br>• where applicable, that the controller intends to **transfer personal data to a recipient in a third country** or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.<br>• **the period for which the personal data will be stored**, or if that is not possible, the criteria used to determine that period;<br>• where the processing is based on point legitimate interest, **the legitimate interests pursued by the entity** or by a third party;<br>• the existence of the **right to request from the entity access to and rectification or erasure of personal data** or **restriction of processing** concerning the data subject and **to object to processing** as well as **the right to data portability**; |

| | | |
|---|---|---|
| | | • where processing is based on data subjects consent, **the existence of the right to withdraw consent at any time**, without affecting the lawfulness of processing based on consent before its withdrawal;<br>• the **right to lodge a complaint** with a supervisory authority;<br>• from which **source the personal data originate**, and if applicable, whether it came from publicly accessible sources;<br>• **the existence of automated decision-making, including profiling**, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.<br>*If the personal data are to be used for communication with the data subject, the above information has to be provided to the data subject the latest at the time of the first communication to that data subject or if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.*<br>The entity has **documented the relevant exception that might apply** for each information not provided by the entity to the data subject. (Art- 14-5) |
| **II-a-12** | Up to date information<br>(GDPR Article 12)<br>(Recitals 58, 61) | For each processing activity in scope, the entity has implemented measures to ensure that:<br>• **relevant changes to the processing activity are identified and communicated** timely to the data subjects. |
| **II-a-13** | Form of information<br>(GDPR Article 12)<br>(Recitals 58, 61) | For each processing activity in scope, the entity has implemented measures to ensure that:<br>• any information addressed to the public or to the data subject is **accurate, easily accessible and written in plain language** (assessment that the communication is adapted to the targets),<br>• **clear and plain language is used** - the entity is able to demonstrate that information is given to the data subjects in an easily accessible way when it is most useful before the processing takes place;<br>• where **communication with children** takes place, such information is addressed in a clear and plain language that the child can easily understand. |
| **II-a-14** | Right of access by the data subjects<br>(GDPR Article 15)<br>(Recitals 63, 64, 73) | For each processing activity in scope, the entity has implemented measures that ensure that it can **effectively implement the "right of access"** by the data subjects. |
| **II-a-15** | Right to data portability<br>(GDPR Article 20)<br>(Recitals 68, 156) | For each processing activity in scope, the entity has implemented measures that ensure that it can **effectively implement the "right to data portability"** of a data subject. |
| **Transfer of personal data to third countries (when applicable)** | | |

| | | |
|---|---|---|
| **II-a-16** | Third country transfers<br>(GDPR Article 46)<br>(Recitals 105, 108, 109, 110, 114) | For each processing activity in scope that involves a transfer of personal data to third countries, the entity has implemented one of the following mechanisms:<br>Mechanisms not requiring any specific authorization from a supervisory authority:<br>• a legally binding and enforceable instrument between public authorities or bodies;<br>• binding corporate rules in accordance with Article 47 of the GDPR;<br>• standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2) of the GDPR;<br>• standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2) of the GDPR;<br>• an approved code of conduct pursuant to Article 40 of the 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<br>• an approved certification mechanism pursuant to Article 42 of the 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.<br>Mechanisms subject to the authorization from a competent supervisory authority:<br>• contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or<br>• provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights. |

## SUBSECTION II –B: PURPOSE LIMITATION

| Ref. | Label | Description |
|---|---|---|
| II-b-1 | Quality of purpose definition<br>(GDPR Article 5)<br>(Recitals 29, 116, 123) | For each processing activity in scope, the entity has implemented measures to ensure that:<br>• it has formally **assessed that the purpose(s)** for which it collects the data are specific, explicit and legitimate;<br>• it does **not further process** the data in a manner that is incompatible with those purposes;<br>• purposes have been described in a way that allows data subjects to understand and assess the impact in regards to their privacy. |
| II-b-2 | Purpose compatibility<br>(GDPR Article 5)<br>(Recitals 29, 116, 123) | For each processing activity in scope, and where processing is using data collected for another purpose, the entity has implemented measures to ensure that:<br>• the processing activities **purpose is compatible with the initial purpose** for which it has been collected. This formal assessment has been approved by management or in case where a DPO has been designated by the DPO. |
| II-b-3 | Automated individual decision-making, including profiling | For each processing activity in scope, the entity has implemented measures that ensure that data subjects can **contest a decision based on automated processing.** |

## SUBSECTION II –C: DATA MINIMISATION

| Ref. | Label | Description |
|---|---|---|
| II-c-1 | Process to ensure data minimization<br>(GDPR Articles 5 and 25)<br>(Recitals 29, 78, 116, 123) | For each processing activity in scope, the entity has implemented measures that ensure that the collection of personal data is adequate, relevant and strictly, limited to what is necessary in relation to the purposes for which they are processed. In particular the entity has assessed that:<br>• It cannot achieve the purpose of its processing activity **with less (privacy invasive)data** (e.g. working with less granular data);<br>• It has **documented the requirement** for each data field in relation to the purpose. |
| II-c-2 | Alternative means<br>(GDPR Articles 5 and 25)<br>(Recitals 29, 78, 116, 123) | For each processing activity in scope, the entity has assessed and documented **the impossibility to reach the purpose(s) in implementing a less intrusive process** (i.e. using less intrusive means). |

## SUBSECTION II –D: ACCURACY

| Ref. | Label | Description |
|---|---|---|
| II-d-1 | Accuracy of the data source<br>(GDPR Article 5)<br>(Recitals 29, 116, 123) | For each processing activity in scope, the entity has implemented measures that ensure that:<br>• **data sources used to collect personal data are relevant**;<br>• collected and processed **data is accurate**. |
| II-d-2 | Updates<br>(GDPR Article 5)<br>(Recitals 29, 116, 123) | For each processing activity in scope, the entity has implemented measures that ensure that:<br>• personal **data is kept up to date**;<br>• **accuracy of personal data is reviewed** on a regular basis – and at least annually. |
| II-d-3 | Right of rectification<br>(GDPR Article 16)<br>(Recitals 39, 59, 65, 156) | For each processing activity in scope, the entity has implemented measures that ensure that it can **effectively implement the "right to rectification"** of a data subject. |
| II-d-4 | Right to restriction of processing<br>(GDPR Article 18)<br>(Recitals 67, 156) | For each processing activity in scope, the entity has implemented measures that ensure that it can **effectively implement the "right to restriction of processing"** of a data subject. |

## SUBSECTION II –E: STORAGE LIMITATION

| Ref. | Label | Description |
|---|---|---|
| II-e-1 | Defined retention period<br>(GDPR Article 5)<br>(Recitals 29, 116, 123) | For each processing activity in scope, the entity has implemented measures that ensure that:<br>• **retention periods are defined** with the input from relevant stakeholders (e.g. legal, business, DPO). The assessment which leads to the retention period is documented, and indicates a clear link between the purpose and the defined period;<br>• **retention periods are communicated by controllers to processors**<br>• **a regular review of the effective implementation** of the defined retention periods is performed – at least annually. Any deviations are duly documented and followed up upon. |

| | | |
|---|---|---|
| **II-e-2** | Right to erasure ('right to be forgotten)<br>(GDPR Article 17)<br>(Recitals 65, 66, 156) | For each processing activity in scope, the entity has implemented measures that ensure that it can **effectively implement the "right to erasure"** of a data subject. |

## SUBSECTION II –F: INTEGRITY, AVAILABILITY AND CONFIDENTIALITY - SECURITY

| Ref. | Label | Description |
|---|---|---|
| **II-f-1** | Risk analysis<br>(GDPR Articles 5, 32)<br>(Recitals 29, 39, 83, 116, 123) | For each processing activity in scope, the entity has implemented measures for the interests of the data subjects that ensure that:<br>• **risks related to confidentiality, integrity and availability are identified, assessed and documented**.<br>• **risk treatment plans** that address those risks are identified, assessed, reviewed, documented and subject to regular review of their effectiveness<br>• **management of the entity is aware of the residual risks** and accepts them.<br>In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. |
| **II-f-2** | Implementation<br>(GDPR Articles 5, 32)<br>(Recitals 29, 39, 83, 116, 123) | For each processing activity in scope, the entity has implemented measures to ensure the **ongoing confidentiality, integrity, availability and resilience of processing systems and services.**<br>*Point of focus: Based on the business practices that can produce a risk on data subjects, the entity has implemented measures which would cover :Asset management; Access control; Cryptography; Physical security; Operations security; Communications security; Security in development; Incident management; Business continuity management*<br>*Point of focus: For each processing activity in scope, the entity implemented state of the **art pseudonymisation and / or encryption** measures of personal data, if appropriate.*<br>*Point of focus: For each processing activity in scope, the entity has implemented measures to **restore the availability and access** to personal data in a timely manner in the event of a physical or technical incident.* |
| **II-f-3** | Testing<br>(GDPR Articles 5, 32)<br>(Recitals 29, 39, 83, 116, 123) | For each processing activity in scope, the entity has implemented a process for **regularly testing, assessing and evaluating the effectiveness of technical and organisational measures** for ensuring the security of the processing |

## SUBSECTION II-G PRIVACY BY DESIGN AND BY DEFAULT

| Data Protection by design and by default | | |
|---|---|---|
| **II-g-1** | Data protection by design<br>(GDPR Article 25)<br>(Recital 78) | The entity has implemented measures that ensure that **data protection principles are integrated** at the earliest possible stage when a new data processing activity is developed.<br>*Point of focus: To demonstrate the implementation of data protection by design reference can be made to the implementation of the certification criteria in this document.* |
| **II-g-2** | Data protection by default<br>(GDPR Article 25)<br>(Recital 78) | The entity has implemented measures that ensure that any **new data processing activity is by default set up in the most privacy friendly/preserving** way for the data subjects.<br>*Point of focus: To demonstrate the implementation of data protection by design reference can be made to the implementation of the certification criteria in this document.* |
| **II-g-3** | DPIA<br>(GDPR Article 35)<br>(Recitals 72, 84, 89, 90, 91, 92, 93, 94, 95) | For each processing activity in scope, the entity has assessed and documented the **decision to perform DPIA**. In case the entity decides:<br>• Not to perform a DPIA, the decision together with the assessment that leads to the decision is approved by the entities management or the DPO in case de entity has designated a DPO.<br>• To perform a DPIA, the DPIA covers at least the following elements:<br>  ○ a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the entity;<br>  ○ an assessment of the necessity and proportionality of the processing operations in relation to the purposes;<br>  ○ an assessment of the risks to the rights and freedoms of data subjects;<br>  ○ the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned. |
| **II-g-4** | DPIA / Prior consultation<br>(GDPR Article 36)<br>(Recitals 37, 94, 95, 96) | For each processing activity in scope, where a **DPIA indicates that the processing would result in a high risk** in the absence of measures taken by the controller to mitigate the risk, the entity has consulted CNPD / the national the supervisory authority prior to the implementation of the processing activity.<br>In case the CNPD / the national the supervisory authority is of the opinion that the intended processing would infringe GDPR, in particular where the entity has insufficiently identified or mitigated the risk, the **entity documents how the written advice that has been provided by CNPD / the national the supervisory authority has been fully addressed** – prior to implement the processing activity. |

## SUBSECTION II-H: OUTSOURCING

| OUTSOURCING | | |
|---|---|---|
| **II-h-1** | Assessment of sufficiency<br>(GDPR Article 28)<br>(Recital 81) | For each processing activity in scope, where the entity uses a processor, it has assessed that the processor is providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements and ensure the protection of the rights of the data subject. |
| **II-h-2** | Contract<br>(GDPR Article 28)<br>(Recital 81) | For each processing activity in scope, where the entity uses a processor, it has a **contract in place** that fulfills the following requirements for the processor:<br>• The processor entity **processes the personal data only on documented instructions** from the entity, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the entity of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;<br>• ensures that persons authorised to process the personal data have committed themselves to **confidentiality or are under an appropriate statutory obligation of confidentiality**;<br>• takes all measures required to **ensure secure processing**;<br>• **Does not engage another processor without prior specific or general written authorisation of the controller**. In the case of general written authorisation, the processor shall inform the entity of any intended changes concerning the addition or replacement of other processors, thereby giving the entity the opportunity to object to such changes. Where a processor engages another processor for carrying out specific processing activities on behalf of the entity, the same data protection obligations as set out in the contract or other legal act between the entity and the processor as shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of GDR.<br>• taking into account the nature of the processing, **assists the controller by appropriate technical and organisational measures**, insofar as this is possible, for the fulfilment of the entity's obligation to respond to requests for exercising the data subject's rights<br>• **assists the controller in ensuring compliance with his obligations** taking into account the nature of processing and the information available to the processor;<br>• **at the choice of the entity, deletes or returns all the personal data to the controller** after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;<br>• **makes available to the controller all information necessary to demonstrate compliance** with the obligations and allows for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. |

| | | |
|---|---|---|
| II-h-3 | Monitoring<br>(GDPR Article 28)<br>(Recital 81) | For each processing activity in scope, where the entity uses a processor, it has defined monitoring and due diligences procedures that ensure that contractual arrangements regarding data protection are satisfied. |

## SECTION III: PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA (PROCESSOR)

| Contracts with the controller | | |
|---|---|---|
| III-1 | Contract<br>(GDPR Articles 28, 29)<br>(Recital 81) | The entity has a **contract with each controller** that fulfills the following requirements:<br>• The entity **processes the personal data only on documented instructions** from the entity, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the entity of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;<br>• ensures that persons authorised to process the personal data have committed themselves to **confidentiality or are under an appropriate statutory obligation of confidentiality**;<br>• takes all measures required to **ensure secure processing**;<br>• **Does not engage another processor without prior specific or general written authorisation of the controller**. In the case of general written authorisation, the processor shall inform the entity of any intended changes concerning the addition or replacement of other processors, thereby giving the entity the opportunity to object to such changes. Where a processor engages another processor for carrying out specific processing activities on behalf of the entity, the same data protection obligations as set out in the contract or other legal act between the entity and the processor as shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of GDR.<br>• taking into account the nature of the processing, **assists the controller by appropriate technical and organisational measures**, insofar as this is possible, for the fulfilment of the entity's obligation to respond to requests for exercising the data subject's rights;<br>• **assists the controller in ensuring compliance with his obligations** taking into account the nature of processing and the information available to the processor;<br>• **at the choice of the entity, deletes or returns all the personal data to the controller** after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;<br>• **makes available to the controller all information necessary to demonstrate compliance** with the obligations and allows for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. |

| | | |
|---|---|---|
| **III-2** | Guarantees<br>(GDPR Article 28)<br>(Recital 81) | The entity has put in place a **documentation of the relevant guarantees** that it can provide to data controllers. The documentation must allow a data controller to assess sufficiency of the guarantees for the processing activities related to him. |
| **III-3** | Limitation<br>(GDPR Article 28)<br>(Recital 81) | The entity has implemented measures to ensure that processing of personal data for his contractual partner (i.e. controller or processor) is limited to those part of **documented instructions from the latter except a legal obligation to do so (check exceptions)** |
| **III-4** | Documented instructions<br>(GDPR Article 28)<br>(Recital 81) | The entity has implemented measures to ensure it is able to demonstrate that **each processing activity is performed on base of a documented instruction from the controller**. |
| **III-5** | Processing without instructions<br>(GDPR Article 28)<br>(Recital 81) | The entity informs the controller in case of a **legal obligation to process, without prior controller's instructions**, the controller's data. |
| **Subcontracting** | | |
| **III-6** | Subcontracting<br>(GDPR Article 28)<br>(Recital 81) | For each processing activity in scope, the entity has **implemented measures to ensure that in case it intends to subcontract the processing activity**, entirely or partially, to another processor:<br>• it obtains prior authorization from all involved level -1 contractors;<br>• In case a general authorization is in place, the entity informs all contractors about the new subcontracting and provide them with opportunity to refuse it;<br>• It has assessed that the subcontracted entity offers the same level of guarantees than the entity provides to its contractors;<br>• It has put in place a contract that ensures the same obligations in regards to data protection requirements than with its initiating contractual partner. |
| **Security** | | |
| III-7 | Risk analysis<br>(GDPR Article 32) | For each processing activity in scope, the entity has implemented measures for the interests of the data subjects that ensure that:<br>• **risks related to confidentiality, integrity and availability are identified, assessed and documented**. |

| | | |
|---|---|---|
| | (Recitals 39, 83) | • **risk treatment plans** that address those risks are identified, assessed, reviewed, documented and subject to regular review of their effectiveness<br>• **management of the entity is fully aware of the residual risks** and accepts them.<br>In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. |
| **III-8** | Implementation<br>(GDPR Article 32)<br>(Recitals 39, 83) | For each processing activity in scope, the entity has implemented measures to ensure the **ongoing confidentiality, integrity, availability and resilience of processing systems and services.**<br>*Point of focus: Based on the business practices that can produce a risk on data subjects, the entity has implemented measures which would cover :Asset management; Access control; Cryptography; Physical security; Operations security; Communications security; Security in development; Incident management; Business continuity management*<br>*Point of focus:*<br>For each processing activity in scope, the entity implemented state of the **art pseudonymisation and / or encryption** measures of personal data, if appropriate.<br>For each processing activity in scope, the entity has implemented measures to **restore the availability and access** to personal data in a timely manner in the event of a physical or technical incident. |
| **III-9** | Testing<br>(GDPR Article 32)<br>(Recitals 39, 83) | For each processing activity in scope, the entity has implemented a process for **regularly testing, assessing and evaluating the effectiveness of technical and organizational measures** for ensuring the security of the processing |
| **Exercise of rights of data subject** | | |
| **III-10** | Data subject rights<br>(GDPR Article 28)<br>(Recital 81) | The entity has documented its **role and responsibilities in regards to the exercise of the following rights towards controllers**:<br>• the right of access,<br>• the right of rectification,<br>• the right of opposition, the right of information,<br>• the right of portability,<br>• the right to be forgotten<br>• the right to contest a decision based on automated processing |

| | | |
|---|---|---|
| **Transfer of personal data to third countries (when applicable)** | | |
| **III-11** | Third countries<br>(GDPR Article 46)<br>(Recitals 105, 108, 109, 110, 114) | For each processing activity in scope, the entity has implemented measures to ensure that one of the following mechanism has been put in place:<br>Without requiring any specific authorization from a supervisory authority:<br>a) a legally binding and enforceable instrument between public authorities or bodies;<br>b) binding corporate rules in accordance with Article 47 of the GDPR;<br>c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2) of the GDPR;<br>d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2) of the GDPR;<br>e) an approved code of conduct pursuant to Article 40 of the 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<br>f) an approved certification mechanism pursuant to Article 42 of the 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.<br>Subject to the authorization from a competent supervisory authority:<br>a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or<br>b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights. |
| **End of the provision of services relating to processing** | | |
| **III-12** | Return / deletion of data<br>(GDPR Article 28)<br>(Recital 81) | The entity has put measures in place to ensure, **at the request of the controller, to delete or to return all the personal data to the controller after the end of the provision of services** relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data |