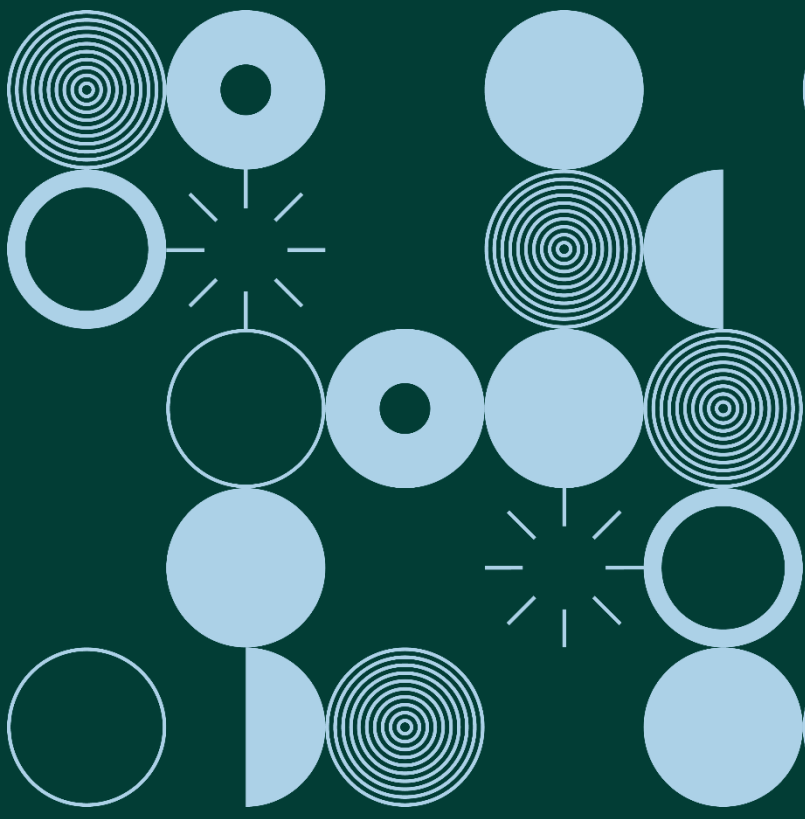
An Coimisiún um Chosaint Sonraí
Data Protection Commission

Guidance Note:

GDPR Certification

September 2020



Contents

Introduction

The General Data Protection Regulation (**GDPR**) seeks to encourage, at European Union level, the demonstration by organisations of their compliance with the provisions of the GDPR. This is set out in Articles 42 and 43 of the GDPR, which deals with data protection certification and allows for organisations to demonstrate and account for any compliance measures in place, while allowing them to enhance and go beyond what is required under the GDPR. Organisations may then be certified as having appropriate safeguards in place for the processing of personal data.

Such measures benefit data subjects as it allows them to quickly assess and understand the level of data protection provided by an organisation's technical and organisational processing operations. Along with GDPR Codes of Conduct, certification is important as it provides a public-facing accountability tool that allows an organisation to demonstrate compliance measures to individuals, as well as to other organisations that it works with, and to supervisory authorities.

A key part of certification is what is commonly known as a "certification scheme". In the context of GDPR, such schemes specify the mechanisms in place for the processing of personal data and how appropriate controls and measures are implemented. These may then be assessed by an accredited certification body. If satisfied, a certification body may then validate and confirm that appropriate controls and measures have been implemented by the organisation and their particular process or service fulfils the scheme's requirements and data protection criteria. The certification body may then certify this is in fact the case. Certified organisations are subsequently reviewed and monitored, by the relevant certification body, to ensure that the criteria continues to be met.

In Ireland, the Data Protection Commission (**DPC**) is the relevant supervisory authority responsible for approval of data protection criteria in certification schemes, while the Irish National Accreditation Board (**INAB**) is responsible for the accreditation of Certification Bodies (**CBs**)[1] that intend operating such schemes.

The following guidance includes:

- a brief description of certification under GDPR and how the DPC will work with INAB, CBs and the European Data Protection Board (**EDPB**) on certification matters,

[1] Sometimes more formally referred to a Conformity Assessment Bodies (CABs)

- a glossary of key definitions and commonly used terms,
- a section with Frequently Asked Questions (FAQ) on particular elements of GDPR certification.

Certification under GDPR

In summary, the GDPR sets out, among other things, that:

- The DPC is required to approve the data protection criteria that will operate within schemes relating to products and/or services that process personal data.
- The scheme criteria will establish, in particular, how processing operations are implemented with regard to assessment and mitigation of risks to personal data and how these satisfy and demonstrate a controller's and/or a processor's compliance with relevant GDPR obligations and their provisions for user rights.
- Certification Bodies (CBs) must be accredited to the ISO-17065/2012 international standard in order to award data protection certification schemes. New schemes can be designed in line with this standard so certification bodies can then achieve this by becoming accredited to such a scheme.
- The GDPR requires that Member States ensure that certification bodies are accredited in accordance with Article 43 of the GDPR. In Ireland, the Irish National Accreditation Board[2] (INAB) are the sole accreditation body who may accredit certification bodies to deliver such schemes with DPC approved criteria.
- The DPC has established a set of "additional requirements" to those already set out in ISO 17065/2012, to be administered by INAB when it accredits CBs that are intending to operate data protection schemes.
- By nature of the ISO-17065/2012 and GDPR requirements, data protection certification schemes are limited in scope to personal data processing operations. This does not preclude the DPC and INAB from working with stakeholders on certification mechanisms for personnel with data protection expertise or obligations, or for tools and management systems related to governance and compliance, but these will not undergo a formal DPC or EDPB approval process.
- Schemes may be designed to operate at a national level, or across the EU (a so-called "EU Seal"), but the latter will require common criteria that account for use in all Member States.
- Organisations may apply to CBs for certification under a particular scheme and use it as a way to demonstrate the compliance of their particular processing operation(s) - the "Target of Evaluation" or "object of certification".
- SMEs in particular may be able to regard suppliers or processors with current and relevant protection certifications as demonstrating compliance of processing operations.

[2] See Section 35 of the Data Protection Act 2018 - http://www.irishstatutebook.ie/eli/2018/act/7/section/35/enacted/en/html#sec35

Certification schemes

In Ireland and other EU member states, currently, there are no fully approved national certification schemes or mechanisms in line with GDPR Arts. 42 and 43. However, the EDPB and all EU supervisory authorities are encouraging stakeholders to create and design such national schemes, as well as EU wide schemes or "seals".

The DPC is working with stakeholders to encourage the establishment of suitable schemes with data protection criteria that it can approve and bring to the EDPB for review and approval. We are currently developing our submission process for the formal approval of GDPR certification criteria. Like other supervisory authorities we have also submitted our additional accreditation requirements for certification bodies to the European Data Protection Board for its opinion. Once we finalise and publish these accreditation requirements for certification bodies and our working agreement with INAB, we will be in a position to accept formal submissions for certification criteria. In the meantime, we welcome enquiries from organisations or other stakeholders who are in the process of developing or have developed GDPR certification criteria. You can find our contact details below.

Once such schemes' criteria are approved and CBs intending to operate the schemes have been accredited, organisations can apply to them to have their processing operations certified. For schemes operated by CBs that are based in Ireland, INAB will perform the accreditation. In the case of EU Seals, accreditation will happen in the member state where the CB makes certification decisions so Irish organisations may seek certification from CBs in other EU member states. Equally, if a CB in Ireland operates an approved and accredited EU Seal, it may then work to certify organisations outside of Ireland. Presently however, there are no approved EU Seals.

Definitions

Many terms used in the EDPB guidelines and in ISO standards documents are defined in the ISO 17000 document. Other ISO standards maintain their own definitions.

- **2018 Act:** the Data Protection Act 2018, which gives further effect to GDPR in Ireland.

- **Accreditation:** third-party attestation related to the activities of a certification body. This is the result of the assessment process for successful certification body (as part of the accreditation process).

- **Accreditation body**: a body that performs accreditation. In this document and for Ireland, this term is taken to mean INAB.

- **Applicant:** an organisation that has applied to have their processing operations certified.

- **Certification:** the assessment and impartial, third-party attestation that the fulfilment of certification criteria has been demonstrated in respect of a controller and/or processor's processing operations.

- **Certification body (CB):** a third party conformity assessment body (**CAB**) operating certification schemes.

- **Certification criteria:** the criteria against which an organisation's processing operations are measured for a given certification scheme.

- **Certification mechanism:** an approved certification scheme which is available to an applicant. It is a service provided by an accredited certification body based on approved criteria and assessment methodology. It is the system by which a controller and/or processor can become certified.

- **Certification scheme:** a certification system related to specified products, processes and services to which the same specified requirements, specific rules and procedures apply. It includes the certification criteria (including GDPR data protection criteria), relevant and applicable standards, and assessment methodology.

- **Client:**[3] an organisation that has been certified (previously the applicant) by the certification body.

- **Competent supervisory authority (CSA):** The GDPR supervisory authority that monitors and enforces the applications of GDPR on its territory. Data protection criteria in schemes are submitted to a CSA for approval.

- **DPC:** Data Protection Commission – Ireland's supervisory authority in relation to the GDPR.

- **General Data Protection Regulation (GDPR):** Regulation EU/2016/679 on the protection of natural person's personal data processing.

[3] Whenever the term "client" is used in this International Standard (ISO/IEC 17065/2012), it applies to both the "applicant" and the "client", unless otherwise specified.

- **ISO 17065**: ISO/IEC 17065/2012 is the conformity assessment standard that specifies the requirements for bodies certifying products, processes and services.

- **National accreditation body (NAB**): the sole body in a Member State named in accordance with Regulation (EC) No 765/2008 of the European Parliament and the Council that performs accreditation with authority derived from the State. In Ireland the NAB is the Irish National Accreditation Board (INAB). INAB is the accreditation relevant body for GDPR certification in Ireland.

- **Scheme owner**: person or organisation responsible for developing and maintaining a specific certification scheme. A scheme owner can be a certification body, a governmental authority, a trade association, a group of certification bodies or others.

- **Target of Evaluation (ToE):** the object of certification. In the case of GDPR certification, this refers to the relevant processing operations that the controller and/or processor is applying to have evaluated and certified. Certification schemes specify requirements[4] for certification of a ToE or object of certification including the processing operations which are determined and assessed for certification.

Contact Us

If you still have questions after reading our guidance and FAQs, email us at certification@dataprotection.ie

Further information

The INAB website contains important information for certification bodies that are or intend to operate in Ireland.

The DPC's website also has other important and relevant information on organisational accountability and other aspects of GDPR

EDPB Guidelines

The EDPB has adopted guidelines on the accreditation of certification bodies under Article 43 of the GDPR (2016/679) and on the operation of certification of organisations and certification criteria under Article 42 and 43.

[4] See for instance sections 4.1 and 6.5 of ISO 17067

The EDPB is expected to publish, in due course, and as per Article 42(2), separate guidelines to address how certification mechanisms can be established as transfer tools to third countries or international organisations.

Other EDPB guidelines on aspects of personal data processing can be found at the EPDB website - https://edpb.europa.eu/our-work-tools/general-guidance_en

Standards organisations

Standards play a significant part in GDPR accreditation and certification and provide an agreed, consistent and expertly considered baseline for certification mechanisms that are operated by CBs.

There are many bodies and organisations around the world that develop standards that may be included in data protection certification schemes that intend to operate in a national or European context. The DPC expects that while data protection certification schemes are likely to be underpinned with Irish, European or International standards, this is not a strict requirement. Some of these are included for reference below.

Irish and European standards organisations

- In Ireland, the National Standards Authority of Ireland (NSAI) is responsible for the development of Irish Standards.
- In Europe, the European Committee For Standardisation (CEN) is an umbrella organisation for 34 European countries standards bodies. CEN works with CENELEC and ETSI as EU recognised bodies for developing and defining standards at an EU level.

International and sectoral

- The United Nations International Telecommunication Union (ITU) work on standards in the telecom sector.
- The Internet Engineering Task Force (IETF) is an internet standards body.
- The World Wide Web Consortium (W3C) develops technical specifications and guidelines for an Open Web Platform.
- In the USA, a government body called the National Institute of Standards and Technology (NIST) provides technology, measurement and standards, including on privacy.

International Standards Organisation - ISO

The International Standards Organisation develop and publish internationally agreed standards. Some published documents by ISO are guidelines, or catalogues of techniques, or principles. Those that have requirements are generally certifiable or may

be included in the basis of a certification scheme or mechanism. The ISO are active in the development of standards related to privacy.

The ISO have recently launched a new standard to help organisations manage privacy – ISO 27701 - but also have many other related standards in various stages of development and completion. The list can be seen at on their website and include some standards that are directly relevant to certification of particular methods of processing operations.

The following may be of particular interest to organisations seeking GDPR accreditation and certification:

- The accreditation standard for products and services – ISO 17065
- The accreditation standard for personnel – ISO 17024
- The accreditation standard for management systems - ISO 17021
- ISO's guidance on developing schemes for ISO 17065 – ISO 17067
- ISO's fundamental accreditation terminology and principles – ISO 17000
- ISO's guidance on developing and specifying criteria or requirements – ISO 17007
- ISO's base standard for accreditation bodies - ISO 17011
- ISOs guide on "common criteria" related to security of products – ISO 15408

Certification FAQs

What is Certification within the meaning of GDPR?

Certification is defined by the International Standards Organisation (ISO) as *"third-party attestation related to products, processes, systems or persons*". This means that an independent assessor decides and attests that specific requirements have been fulfilled, relevant to certification.

In the context of the General Data Protection Regulation (GDPR) certification under Articles 42 and 43 is an accountability tool, with supervisory authority approved data protection criteria, that is limited in scope to processing operations involving personal data.

In Ireland, Certification bodies intending to operate approved data protection certification schemes, are to be accredited by the Irish National Accreditation Board (INAB) in accordance with ISO 17065 and additional requirements established by the Data Protection Commission (DPC).

In the wider context of data protection the regulation also calls on supervisory authorities to encourage certification. For instance, this may be in relation to personnel with data protection expertise for example a Data Protection Officer (DPO) or obligations, or for tools and management systems related to compliance.

EU supervisory authorities will be working on encouraging certification in these areas. For some authorities, it is likely that the initial focus of certification activities will be for stakeholder designed schemes that allow demonstration of processing operation compliance. In any case, whether certification is ultimately for processing operations, personnel or management systems, it is not envisaged as an accountability tool for demonstrating broad or "across the board" GDPR compliance.

What will certification schemes address?

Schemes intended for DPC approval under GDPR Arts. 42 and 43 are to be limited in scope to processing operations and should not be intended for certification of broad 'GDPR compliance', for personnel or for management systems (but may include personnel and management systems as an element of the processing operation).

In particular, certification under GDPR is intended to be used to demonstrate compliance in relation to:

- Article 24 - Responsibility of the controller

- Article 25 – Data protection by design and default
- Article 28 – Data Processor demonstration of guarantees
- Article 32 – Security of processing
- Article 46 – Transfers by way of appropriate safeguards

As such, we might see schemes evolving in the following areas of personal data processing:

- transparency in provision of legitimate interest balancing tests;
- technical system design in big data processing for effective provision of user rights;
- effective credential processing, security and management for authorisation and identity data;
- secure pseudonymisation techniques in medical research processing;
- software testing for data protection requirements in user facing web services;
- record keeping formats and qualities, change control processes and accountability structures for online services handling personal data; and
- effective transparency for algorithms used in public services provision.

What are the benefits of Certification?

Certification is one tool organisations may include when undertaking their GDPR accountability obligations. In so doing they may enhance their processing operations while also demonstrating their compliance measures. These measures may go beyond what is minimally required under GDPR and the Data Protection Act 2018.

As a result, certification may help to enhance transparency for data subjects and business to business relations e.g. between controllers and processor allow for a quicker and more precise assessment and understand the level of data protection of an organisation's products and services. This will serve to build data subjects' trust in the personal data handling performed by certified controllers or processors.

Is Certification a requirement of GDPR?

No. Certification under GDPR is not a requirement or obligation for data controllers or data processers and is a voluntary process. However, an organisation seeking to demonstrate its compliance measures may use certification as a means to achieve that.

Who is involved in certification and what do they do?

Several parties are involved in GDPR certification and accreditation.

- The DPC is Ireland's independent authority responsible for upholding the fundamental right of individuals in the EU to have their personal data protected. It approves data protection criteria in certification schemes, sets requirements for

accreditation of certification bodies and also monitors how those criteria and requirements are applied.

- The Irish National Accreditation Board (INAB) is the agency in Ireland that performs accreditation of certification bodies with authority derived from the State, as per EU regulation 765/2008/EC, and in accordance with the ISO 17000 series of standards and guides.
- The European Data Protection Board (EDPB) is the GDPR established entity, that among other things, applies consistency mechanisms in respect of supervisory authorities, including on decisions related to national and EU Seal certification schemes' criteria.
- Certification Bodies (also known as Conformity Assessment Bodies) are organisations that provide assessment and attestation services for organisations and certify their activities fulfil the requirements that are set out in certification schemes. For GDPR certification schemes, certification bodies do this for schemes that are in line with the ISO 17065 standard.
- Scheme Owners or Designers are stakeholders that develop data protection certification schemes or mechanisms.
- Organisations acting as GDPR data controllers & data processors that seek to have their processing operations certified
- The EU Commission may in future implement or delegate legislation on standards, mechanisms and requirements for GDPR accreditation or certification.

What are 'additional requirements'?

Supervisory authorities that work with National Accreditation Bodies will establish their own additional accreditation requirements for certification bodies seeking accreditation to a data protection scheme. These are requirements which are additional to those already set out in the standard ISO 17065/2012 (and others required by INAB). They are focused on ensuring CBs meet the obligations set out in GDPR Arts. 42 and 43, such as demonstrating:

- expertise in relation to the data protection subject matter to be certified
- procedures for administration of data protection seals and marks
- independence and impartiality from the organisations they are working to certify

DPCs accreditation requirements, which INAB will administer during their accreditation process, are published on our website.

What are the 'criteria' DPC is required to approve?

The criteria are a set of organisational and technical requirements related to a defined scope and "object of certification" (a particular or set of processing operations):

- that are set out in a certification scheme

- that an organisation meets when they put in place their measures and controls
- that are to be assessed and evaluated by a certification body.

The basis for data protection certification criteria are to be derived from the GDPR principles and rules. Further information, is available in the EDPB guidelines that detail what is expected.

Who will develop certification schemes and criteria?

The GDPR allows for various stakeholders, including certification bodies, industry groups and supervisory authorities to develop certification schemes. The DPC expects that certification scheme owners will likely be certification bodies, working with other stakeholders, that will design and develop schemes specifying data protection criteria.

Currently, the DPC itself has no specific scheme under development but we may consider doing so in the future. The current focus for the DPC is ensuring that we and INAB have the processes and systems in place to facilitate GDPR certification.

Certain criteria are to be derived from the GDPR principles and rules which will be characterised by three core elements:

- they should relate to personal data processing
- they should relate to any technical systems used to process the personal data
- they should relate to the process and procedures involved in the personal data processing operation(s)

Annex 2 of the Guidelines 1/2018 provides guidance for review and assessment of certification criteria. It identifies topics that a data protection supervisory authority and the EDPB will consider and apply for the purpose of approval of certification criteria of a certification mechanism.

To whom/where does a scheme owner or certification body apply for GDPR certification scheme approval?

The choice of where to submit an application for approval of criteria will be based on the location of the certification scheme owner and their stakeholder role. Details of this are being finalised with INAB (who usually deal with CBs), so scheme owners should check with INAB and DPC beforehand.

- Scheme owners who are CBs should formally submit their schemes and applications to INAB. INAB will inform DPC of this and DPC will commence work to assess data protection criteria.
- Scheme owners who are not CBs should submit their schemes and applications to DPC. The DPC will inform INAB.

In both case preliminary requirements will be checked and if a scheme or criteria are clearly not suitable for assessment it may be returned to the owner. An application form will be made available once this process is finalised.

What is the significance of an EU Seal?

Data protection certification schemes may be intended and designed for either national or EU usage. Those intended to be used across the EU may become known as '*EU Seals*' if approved by the EDPB.

If the certification scheme and criteria are intended for EU-wide use, then the criteria need to be customisable in a manner that will take account of any applicable national sector specific regulations or local requirements.

All such schemes' criteria will need to be assessed by the concerned national data protection authority for validation and approval and subsequently by the EDPB for consideration under the GDPR consistency mechanism.

How is it possible to know whether an organisation's processing or service is certified?

Generally you are likely to find this information on the organisation's website. Accredited certification bodies will likely also keep an up to date list of organisations they have certified, the scope of their certification (what service or process has been certified), and details of when the certification was awarded and will expire.

The DPC will publish its accreditation requirements and the details of any scheme criteria it approves (as will the EDPB).

Does certification mean that an organisation is compliant with GDPR?

No. Certification is an accountability mechanism that allows a data controller to demonstrate, with accredited certification body assessment and evaluation, that certain aspects of a processing operation and any associated risk mitigation measures, are intended to be compliant with GDPR.

As a result, it is important to remember that certification does not actually mean that an organisation's processing operation is definitively compliant under GDPR. It is only when and if a supervisory authority examines a processing operation that a determination of compliance with GDPR can be made.

What is the difference between "GDPR certification" and other certification?

Certification under GDPR involves an accredited certification body assessing an organisation's processing operation under a certification scheme involving criteria that has been approved by the relevant supervisory authority and the EDPB.

Other certifications related to personal data can be performed by accredited certification bodies under schemes that do not have supervisory authority approved criteria where they relate to matters other than processing operations or services. For example, such schemes may address the qualifications and experience of personnel, such as a data protection officer or a management system that defines policies and procedures for an organisation's activities.

It is also possible to achieve other kinds of certification by different organisations in conjunction with other standards agencies, but these may not involve or require the oversight and assurance of INAB accreditation.

What is ISO/IEC 17065/2012?

Article 43 of GDPR obliges EU member states whose data protection authority will not perform accreditation themselves to ensure that certification bodies with expertise in data protection are accredited by a national accreditation body using the ISO 17065 standard.

In Ireland, INAB is responsible for this accreditation and the DPC is responsible for defining the additional requirements INAB will apply to such certification bodies.

ISO 17065 is an international standard for CBs that intend to certify products, processes and/or services as defined by specific certification schemes or mechanisms. It sets out:

- **general requirements**, including legal and contractual matters, management of impartiality, liability and financing, non-discriminatory conditions, confidentiality and publicly available information;
- **structural requirements**, including organisational structure and top management and a mechanism for safeguarding impartiality;
- **resource requirements**, including certification body personnel, resources for evaluation activities and outsourcing;
- **process requirements**, including application, application review , evaluation, review, certification decision, certification documentation, directory of certified products, surveillance, changes affecting certification, termination, reduction, suspension or withdrawal of certification, records, and complaints and appeals;

- **management system requirements** – including options for general management system documentation, control of documents, control of records, management review, internal audits, corrective actions and preventive actions.

Under the GDPR, where a Member State's supervisory authority will not perform accreditation themselves, they will specify additional requirements that their NAB shall apply to certification bodies seeking accreditation for operating a data protection scheme. The certification scheme sets out the following parameters:

- the specific product, process and/or service to be certified – in GDPR terms, this can be seen as a "processing operation"
- the specified requirements (e.g. standards) that the product, process and/or service must fulfil;
- sampling criteria for the target processing operation that is to be certified;
- types and combinations of conformity assessment techniques (e.g. audit, inspection or test) that will be used to evaluate the product, process or service;
- the process to be followed for the evaluation, review and decision;
- the mark of conformity and its control;
- activities that must be undertaken during surveillance, if any.

Under the GDPR, data protection certification schemes are required to have criteria that a data protection supervisory authority or EDPB is required to approve.

The following ISO documents provide guidance on how to establish and manage certification schemes for products, processes and services:

- ISO/IEC 17067:2013, *Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes*
- ISO/IEC 17026, *Conformity assessment — Example of a product certification scheme, contain guidance on how to establish and manage certification schemes for products, processes and services.*
- ISO 17007, *Conformity assessment — Guidance for drafting normative documents suitable for use for conformity assessment*

Annex 2 of the EDPB Guidelines 1/2018 provides guidance for review and assessment of certification criteria. It identifies topics that a data protection supervisory authority and the EDPB will consider and apply for the purpose of approval of certification criteria of a certification mechanism.

The EDPB has also adopted guidelines on the accreditation of certification bodies under Article 43 of the GDPR (2016/679)