GDPR Certification Standard and Criteria

BC 5701:2023

> the new standard in GDPR compliance

A white paper by

Brand Compliance

piims academy

Colophon

This whitepaper is published by:

Text and editing

Piims Academy BV
Core author BC 5701
www.piims.nl

Brand Compliance BV
Certifying institution BC 5701
www.brandcompliance.com

Design

Purple Media BV
Design, development & online marketing
www.purplemedia.nl

Printing

Drukwerkdeal
Online printing
www.drukwerkdeal.nl

Content

Disclaimer

This white paper is intended to provide interested parties with a general overview of the GDPR certification standard BC 5701. For the sake of clarity, we sometimes outline a simplified representation of reality. Therefore, no rights can be derived from this white paper.

GDPR Certification Standard and Criteria

BC 5701

The new standard in GDPR compliance

After years of development, the BC 5701 has recently reached an important milestone: approval by the Autoriteit Persoonsgegevens (AP); the Dutch Supervisory Authority. This means that the AP has decided that the application of the BC 5701 leads to a demonstrably appropriate elaboration of the GDPR. This whitepaper provides information on the structure, background and content of the certification standard. We outline the approval process, explain what approval entails and show how organisations can benefit from this new standard.

The value of GDPR certification

Before we get into the details of the BC 5701, let's take a quick look at the value of GDPR certification. In other words, who is it for and what solution does it provide? We will do this from two perspectives. Firstly, the value to society and then the value to the organisation being certified.

The value to society

One of the main driving forces behind GDPR legislation is to ensure economic growth within the European Union[1]. Driven by rapid technological developments, products and services are becoming increasingly complex and digital. It is not uncommon for even professionals to be unable to fully understand the products and processes they are purchasing. This means that trust is becoming increasingly important in economic transactions. The key question is: what can form a good basis for this trust? After all, thanks to the credit crisis, we all know what the consequences of unfounded trust can be.

[1] See recitals 6 and 7 GDPR.

The BC 5701 is designed to contribute to societal trust in a number of ways. First, the BC 5701 gives the concept of 'GDPR compliance' hands and feet; it explains how GDPR compliance can be achieved. For example, it helps organisations give real meaning and substance to compliance agreements with controllers and/or processors. Second, the BC 5701 promotes proper implementation of the GDPR, which in turn directly contributes to better protection of personal data. Thirdly, the BC 5701 logo provides all stakeholders with an at-a-glance assurance of the integrity and quality of personal data processing. Last but not least, the BC 5701 helps to improve the protection and control of data subjects' personal data through its implementation requirements. In short, GDPR certification demonstrates the trustworthiness of the processing of personal data.

The value for organisations seeking certification

Any organisation that is serious about protecting personal data will face the same kind of problems when elaborating the GDPR, regardless of the size of the organisation, the complexity of the processing, or the GDPR-role of the organisation. These problems are related to the abstraction of the law. Below we explain three common issues and outline how the BC 5701 helps organisations to address them.

The appropriateness of the elaboration

The appropriateness of the elaboration has to do with the specific processing context of the organisation and the question of when the elaboration is good (enough). The BC 5701 helps organisations to answer this question by indicating exactly which aspects the organisation should take action on and what the action should be. It also helps the organisation to determine whether the actions taken are adequate.

The GDPR compliance of external parties

Every organisation uses processors. The challenge is that the organisation does not have operational control over these activities, but is responsible for them. How does the organisation consistently and adequately assess the GDPR compliance of processors, and in doing so, how does the organisation keep a grip on the costs in the process? After all, serious assessment requires serious capacity.

The BC 5701 contributes to the solution in two ways. Firstly, it provides the certifying organisation with concrete tools to properly assess their processors. Secondly, it enables processors to proactively demonstrate their GDPR compliance to their customers. As a result, processors can offer their customers peace of mind, save them time and reduce the cost of partnership.

Demonstration of one's own compliance

Perhaps even more important than the legal requirement to demonstrate GDPR compliance, is the fact that many organisations want to demonstrate their GDPR compliance. To be credible, a compliance pitch must meet three conditions:

1. Compliance is established against clear criteria (verifiability);
2. The assessment has been carried out by an independent party (objectivity);
3. The assessment is of sufficient quality (reliability).

The BC 5701 is designed to provide indisputable evidence of GDPR compliance in relation to a processing operation to all stakeholders of that processing operation.

Key benefits of GDPR certification

Towards stakeholders

- Provides confidence in a black-box process
- Improves control over own data
- Reduces risks of doing business

Towards Clients

- Lower partnership costs
- Saves monitoring time
- Provides peace of mind

Towards society

- Contribute to trust in the digital economy
- Promote correct application of the GDPR

For its own organisation

- Demonstrate quality and integrity of processing to all stakeholders
- Actively support the image of a reliable and progressive organisation
- Improve process control
- Take the initiative in terms of accountability (for processors)
- Reduce processing risks

The structure of the BC 5701

The BC 5701 is essentially made up of three building blocks. The first building block is the GDPR itself. Or rather, the requirements imposed by the GDPR. For some of these requirements, those relating to the adequate protection of personal data, it relies on existing Information Security (IS) standards. These are the second building block. The third and final building block is a management system, added to ensure future compliance. Together they form the three building blocks of BC 5701. They are explained below.

Building block: GDPR

The GDPR requires that GDPR-certification is based on ISO 17065. This requirement has a significant impact on the certification process. This is because ISO 17065 contains requirements with respect to the certification of products, processes and services. This is very different from well-known certifications such as ISO 9001 (quality) and ISO 27001 (information security). These are management system certifications. The table on page 6 shows an example of the difference between the two. Below we discuss the implications for the certification process.

The fact that the BC 5701 is essentially a form of product certification means that three aspects are significantly different from what one would expect from experience with management system certification.
First, the GDPR (the source of the certification requirements) aims to protect the interests of data subjects. This automatically makes the BC 5701 perspective that of the data subjects. So it is not the organisation's interests that come first, but the data subjects' interests; the organisation's interests come second.
Secondly, the certification focuses on the processing operations and not on the organisation as a whole. There is therefore a need to clearly delineate what is covered by certification and what is not.
Thirdly, certification requirements are more specific and certification audits more thorough and rigorous than organisations may be used to from certifications. For example, all or virtually all processors are assessed to determine whether the suitability of the processor has been established; whether all processing and protection requirements have been correctly agreed; whether compliance with the agreement is consistently and adequately monitored; and whether appropriate action is taken in the event of non-compliance.

In other words, the certification audit aims to provide a high level of assurance that all aspects of the GDPR are being implemented correctly on an ongoing basis and that their quality is being assured.

Building block: IS (Information Security) **standard**

One of the principles of the GDPR is “integrity and confidentiality”. This requires organisations to take adequate technical and organisational measures to protect personal data. This is the domain of information security and there are already a number of best practices that have been proven to be adequate. For BC 5701, it was therefore decided not to reinvent the wheel, but to link to established standards for information security. For organisations seeking certification, this means that they must also comply with an appropriate information security standard.

The IS standard must then be linked by the organisation to the BC 5701. The emphasis here is on the difference in perspective described above. Information security standards focus on protecting the interests of the organisation. GDPR certification focuses on the interests of the data subjects. Linking means that the organisation must demonstrate that the technical and organisational measures are suitable to avoid or adequately reduce the risks to the data subjects.

Building block: Management system

As mentioned, GDPR-certification is essentially a form of product certification. Its purpose is to test whether a processing of personal data meets the requirements of the GDPR. Our experience has shown that such a process focus does not meet the needs of all stakeholders. A key reason for organisations to seek certification is to gain the trust of their stakeholders. To gain this trust, the certificate should not only tell something about the proper processing and protection before and at the time of the audit (historical perspective), but also about the organisation's ability to continue to comply (future perspective). So, to meet the expectations of all stakeholders, the third building block, the management system, was added. The management system ensures that the organisation continues to implement ongoing changes within and outside the organisation in line with the GDPR.

Product certification versus management system certification

Subject	Product certification	Management system certification
The requirement	A car tyre of type X, shall be able to drain Y litres of water per second at a speed of Z km/h.	The organisation shall systematically determine that the tyres produced meet the quality requirements defined by the organisation.
Characteristics of the requirement	▪ Relates directly to the car tyre (the product); ▪ is specific (externally defined).	▪ Relates to the management of the production process (is indirect); ▪ is general (depends on the organisation's own standards).
Audit	Determines with a specified degree of certainty and accuracy whether all car tyres meet the specified requirements. **Base:** statistically valid sampling	Determines whether the organisation executes its own policies in accordance with the design. **Base:** judgement based sampling
Meaning of conformity	The organisation produces car tyres of a certain quality.	The organisation controls its production process. (It cannot be said that this manufacturer produces good car tyres, because that depends on the quality requirements they impose on themselves, which the organization can change at any time.)

A simplified example of the difference between product certification and management system certification for a car tyre manufacturer.

Suitable for whom and what

Of course, the BC 5701 can be used in any country, but its approval relates to the Dutch market. In other words, for organisations based in the Netherlands, in relation to processing operations that take place in the Netherlands and (at least) targeted at data subjects located in the Netherlands. Within this, the BC 5701 can be applied to any processing of personal data, regardless of the sector in which it takes place and regardless of the processing role the organisation has. The essence is this:

1. the certification relates to a one or more processing operations;
2. the organisation is a (joint) controller or processor with regard to the processing.

Thus, certification always refers to one or more processing operations performed by an organisation in a specific GDPR capacity. Therefore, it is not possible to certify a product with the BC 5701. Take for example a smart fridge. The fridge itself cannot be certified, but the processing of personal data offered as a service with this fridge can be certified.

The Target of Evaluation

Central to a certification process is the collection of processing operations that the organisation wishes to certify. In the BC 5701, this collection is called the 'Target of Evaluation'. When determining this, it is important to keep in mind the purpose of the processing for the primary stakeholders of the certification. After all, it is all about building trust with the data subjects and/or customers. The Target of Evaluation should therefore be meaningful to the primary stakeholders. This means that the certification has to cover all processing operations that are related to the processing purposes of the primary stakeholders. Only then will the certification be of value to them. Defining the Target of Evaluation is the logical starting point for any BC 5701 implementation proces.

The scope of certification

The Target of Evaluation determines which processing operations will be certified. The scope then describes all aspects of the organisation that affect the Target of Evaluation. As part of the certification, it is necessary to ensure that these aspects are also implemented in accordance with the GDPR. This includes the development or modification of the processing operations, the infrastructure for carrying out the processing, the policies that set the framework for to the processing, the employees involved in the different stages of the processing, and so on. Thus, although the certification focuses on a set of processing operations, the certification process involves many more aspects of the organisation.

The contents of the BC 5701

This chapter gives you an overview of what you will find in the Certification Standard. The BC 5701 consists of 10 chapters. These are briefly described below.

Introductory chapters

BC 5701 starts with 4 introductory chapters; these do not contain implementation requirements.

Introduction

The introduction describes the structure of the BC 5701. It explains how to read the BC 5701.

1 - Topic

Gives a brief description of the subject of the BC 5701. It has no practical significance.

2 - Normative references

A short but important chapter. It describes which laws and regulations, in addition to the GDPR and the BC 5701, must be taken into account to qualify for certification.

3 - Definitions

As the title suggests, this chapter contains the definitions of the terms used and the meaning of the abbreviations and symbols used.

Chapters with implementation requirements

Chapters 4 to 9 describe the measures organisations must implement to be considered for certification. Within each chapter, the topics are always presented in the same way. First there is a description of the (GDPR) context, followed by an objective to be achieved. The objective is then translated into implementation criteria to achieve the objective. Each section concludes with the applicable articles and recitals of the GDPR.

Each objective and implementation criteria indicates whether it applies to controllers, processors or both.

4 - Context of the processing

In this first chapter of implementation requirements, the organisation is asked to describe the internal and external context of the processing. In addition, this chapter identifies all external and internal requirements and translates them into processing requirements. Finally, this chapter deals with the necessary delineation of the application of the BC 5701.

5 - Organising the data protection

Chapter 5 deals with all aspects that should be addressed at the organisational level, rather than at the processing level(s). These include management involvement, personal data protection policies, requirements for the DPO and the records of processing activities.

6 - Fundamentals of the processing activities

Chapter 6 focuses on the design of the processing. This includes mapping the processing, elaborating on the principles of the GDPR and documenting the processing chain.

7 - Technical and organisational protection

Once the design of the processing operations has been determined, Chapter 7 deals with the aspects that support the processing and protection of personal data. It contains the requirements related to the information security standard, deals with risk management from the perspective of the data subjects, data protection by design and by default, and addresses aspects to be covered with regard to the personnel involved.

8 - Operational execution

This penultimate chapter brings together all the requirements that come into play when processing becomes operational. Topics covered here include: the rights of the data subjects, dealing with processors, transfers of personal data, data breaches and monitoring changes in the context of processing.

9 - Management system

Finally, Chapter 9 describes the management system to be implemented by the organisation. The management system aims, on the one hand, to continuously monitor and improve the quality of data processing. On the other hand, it ensures that the organisation implements changes related to processing in accordance with the GDPR.

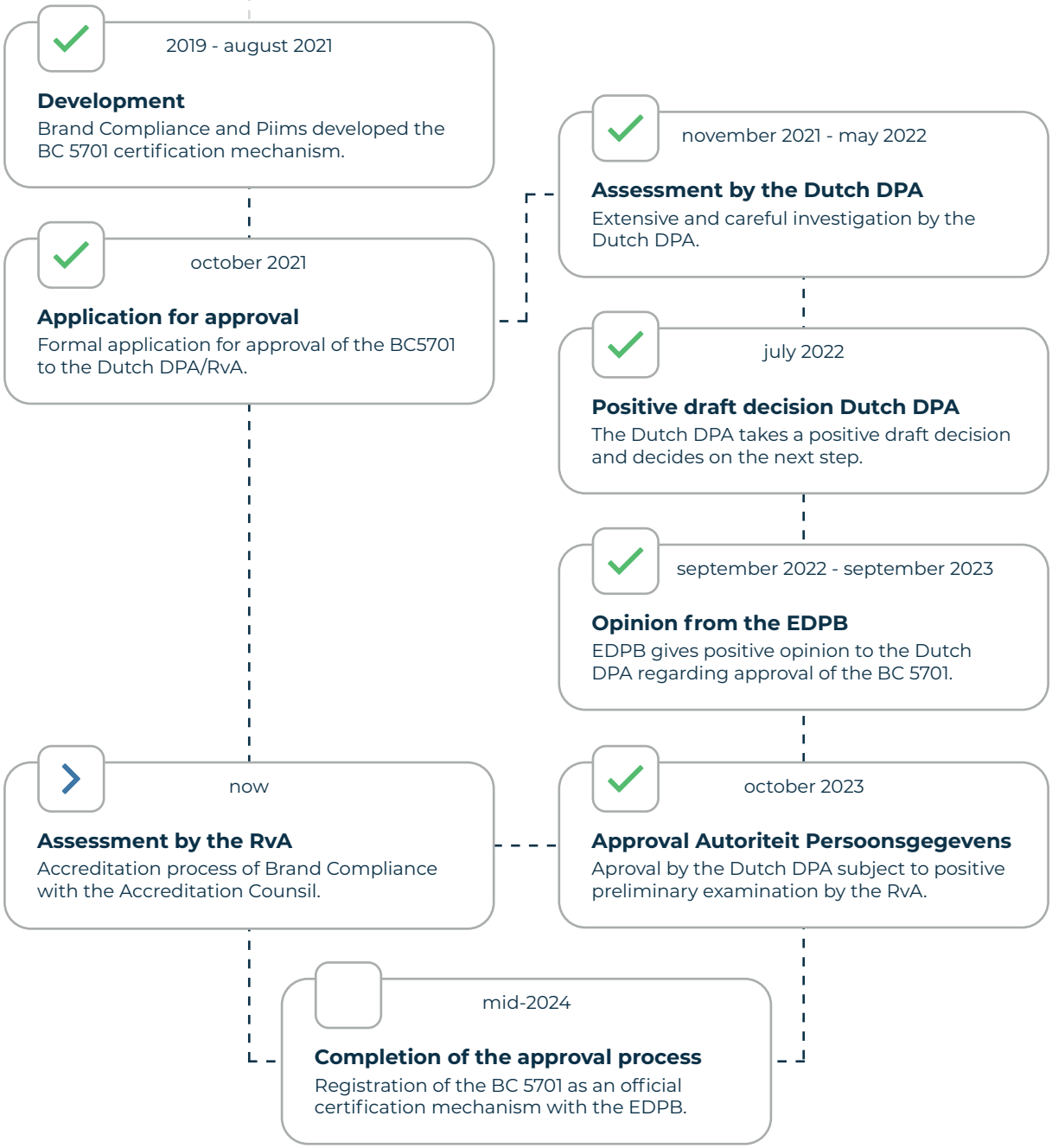
Appendices

Finally, there are three informative overviews to help organisations apply the certification standard.

1. Overview of documentation requirements
2. Cross-reference table GDPR to certification criteria
3. Relevant guidelines from the EDPB and the Autoriteit Persoonsgegevens

The approval process of the BC 5701

In October 2023, after an extensive national and European review process, the Dutch Data Protection Authority approved the GDPR Certification Standard and Criteria BC 5701:2023. This means that the Dutch DPA is of the opinion that the application of the standard leads to a demonstrably adequate elaboration of the GDPR. The approval process is outlined below. Future timeframes are estimates based on our experience to date.



The BC 5701, (not) for every organisation

Any organisation that processes personal data can start working with the BC 5701. The standard can be used in two ways:

1. as a (non-binding) guideline to establish GDPR compliance, or
2. as a tool to prepare for certification.

Prerequisite for successful certification

If reading this white paper has got you this far, you may be considering certification. If so, we would like to point out another important aspect of GDPR certification. This is the place within the organisation where you ensure GDPR compliance. Our advice is to organise the protection of personal data as a quality aspect of the primary business activities, not as a responsibility of the support staff. Ensuring GDPR compliance as part of core business activities ensures that it is always a point of attention, and not just when the supporting staff points it out to the organisation. It also ensures that even certification audits do not reveal any surprises and 'just' become a cause for celebration!

Now is the time to act

As mentioned, we can't say exactly how long the accreditation of Brand Compliance will take. But don't let that stop you from starting your implementation now. In fact, for an average implementation process, you should expect a lead time of six to twelve months. So do you want to be one of the first organisations in the Netherlands (and Europe) to be GDPR-certified? Start your implementation process now.

Guide to certification

The GDPR-Certification Standard and Criteria BC 5701:2023 contains the requirements for organisations to qualify for certification.

The standard comprises over 180 pages and is in Dutch and English as PDF available at www.brandcompliance.com for € 245,- excluding VAT.

Implementation and certification

When you are considering certification, you will of course want to know what the process will mean for your organisation. In this chapter, we outline the implementation process.

GAP analysis

It's most likely that your organisation has already done a lot of work towards GDPR compliance. The question is: What steps still need to be taken to comply with the GDPR, and what are the implications? This requires a GAP analysis, which can be done in roughly three ways:

1. Do it yourself after studying the Standard;
2. Do it yourself after training as a BC 5701 Implementation Professional;
2. Have Brand Compliance do it.

Experience has shown that the impact of the BC 5701 is easily underestimated. We therefore recommend that you choose option two or three. After all, you don't want to wait until the certification audit to find out what the BC 5701 implementation requirements really mean for your organisation. This will lead to unnecessary rework, unnecessary costs and a significant delay in the certification process.

Implementation

Depending on the complexity of the processing context, the maturity of the organisation and the resources available, your implementation will take an average of six to twelve months.

To best prepare you for the implementation process, we now offer several training courses for different roles involved in the implementation. Participants will learn to understand and apply the critical elements of BC 5701. See the next chapter for more information.

Operationalization and internal audit

Once implementation is complete, the organisation shall determine that all technical and organisational measures implemented are working as intended. This is part of the management system. The determination is made by an internal audit followed by a management review. All technical and organisational measures must have been fully operational for at least three months in order to conduct a meaningful certification audit.

Certification

The certification audit is carried out by a multidisciplinary audit team that includes legal, technical and organisational expertise. Depending on the organisation's processing context, the audit team may be extended to include supporting specialists. The legal auditor focuses on assessing the legality aspects. The technical auditor focuses on the technical implementation of the processing and protection of personal data and a number of technical aspects related to accountability. Finally, the lead auditor focuses on the organisational aspects of implementation and coordinates the audit.

Continuation of certification

On successful completion of the certification process, the BC 5701 certificate is issued. This certificate enables the organisation to demonstrate that:

- the relevant processing of personal data is carried out in accordance with the GDPR, and
- that the organisation implements changes in accordance with the GDPR.

The BC 5701 certificate is valid for three years. During these three years, the organisation must continue to demonstrate that it is operating in accordance with the requirements. This is assessed annually by Brand Compliance through so-called 'surveillance audits'. Surveillance audits are also carried out by a multi-disciplinary audit team. The surveillance audits determine whether the organisation has operated in accordance with the certification criteria during the previous period and whether the organisation has responded correctly to changes in the context of the certified processing operations.

A certification cycle therefore consists of an initial audit and two surveillance audits. At the end of the three-year period, the organisation can opt for recertification, in which case the cycle starts again.

The BC 5701 certificate makes the quality and integrity of your data processing visible to all stakeholders.

The organisations behind the BC 5701

The BC 5701 certification mechanism is a joint development of Brand Compliance and Piims Academy. Below we briefly explain who you can contact for which topics.

Brand Compliance

Brand Compliance is a certification body that conducts accredited certification audits in the areas of quality, information security and privacy. With regard to the BC 5701, Brand Compliance is the owner of the certification scheme and also the certifying body. Brand Compliance is the point of contact for the following topics,:

- Gap analyses related to the BC 5701
- Participation in pilot projects
- Certification audits

For further information please visit: www.brandcompliance.com

Brand Compliance cannot provide internal audits/reviews or other consultancy services to clients for whom certification activities are performed.

piims academy

Piims Academy is the principal author of the 'GDPR Certification Standard and Criteria BC 5701:2023' and uses this knowledge to help people and organisations implement the GDPR in a demonstrably appropriate manner. Piims Academy develops and provides all official BC 5701 training courses.

Do you have the ambition to make (your) organisation(s) stand out in the processing of personal data? On the following page you will find the courses that can help you do just that.

The following courses are available (in Dutch) through Piims Academy:

BC 5701 for decision-makers

- Duration: 1/2 day
- Explore the key opportunities and challenges of the Standard
- For: Decision-makers

BC 5701 Counselor

- Duration: 3 days
- Learn to advise correctly and adequately with regard to the BC 5701
- For: Legal advisers

Implementation Professional (FT)

- Duration: 6 days (Fast Track)
- Certification-worthy implementation for experienced implementation managers
- For: Consultants

Implementation Professional (AL)

- Duration: 10 days (Applied Learning)
- Parallel learning and implementation with feedback on your implementation
- For: Product owners, Project managers

BC 5701 Internal Auditor

- Duration: 4 days
- For Implementation Professionals who want to audit or further deepen their knowledge
- For: Auditors and Consultants

BC 5701 Benchmark

- Duration: 4 days
- Learn to use the Standard as a benchmark for the adequate application of the GDPR
- For: Privacy professionals

More information on training and support can be found at: www.piims.nl

Brand Compliance

www.brandcompliance.com
info@brandcompliance.com

piims academy

www.piims.nl
info@piims.nl