Brand Compliance

CERTIFICATION REGULATIONS BC 5701

Contents

1 Introduction

As a certification body (CB), Brand Compliance provides services related to audits on 'the application of the GDPR when processing personal data by controllers and/or processors'. The process is certified under the GDPR Certification Standard and Criteria BC 5701:2024 based on the Certification Scheme BC 5701:2024.

Brand Compliance strives for certification carried out under accreditation in accordance with the rules of the national accrediting body. Information regarding Brand Compliance's current accreditations can be found on the website of the Dutch Accreditation Council.

In the following text, the organisation seeking certification of its processing(s) is referred to as 'the organisation' and Brand Compliance B.V. as 'Brand Compliance'.

1.1 Scope

These Certification regulations apply to the following standard:

- ✓ GDPR Certification standard and criteria BC 5701:2024 (from here on referred to as BC 5701)

1.2 Purpose of these Certification Regulations

The purpose of these Certification Regulations is to provide all organisations with an understanding of the way of working, procedures and the agreements applicable to them.

2 Certification process

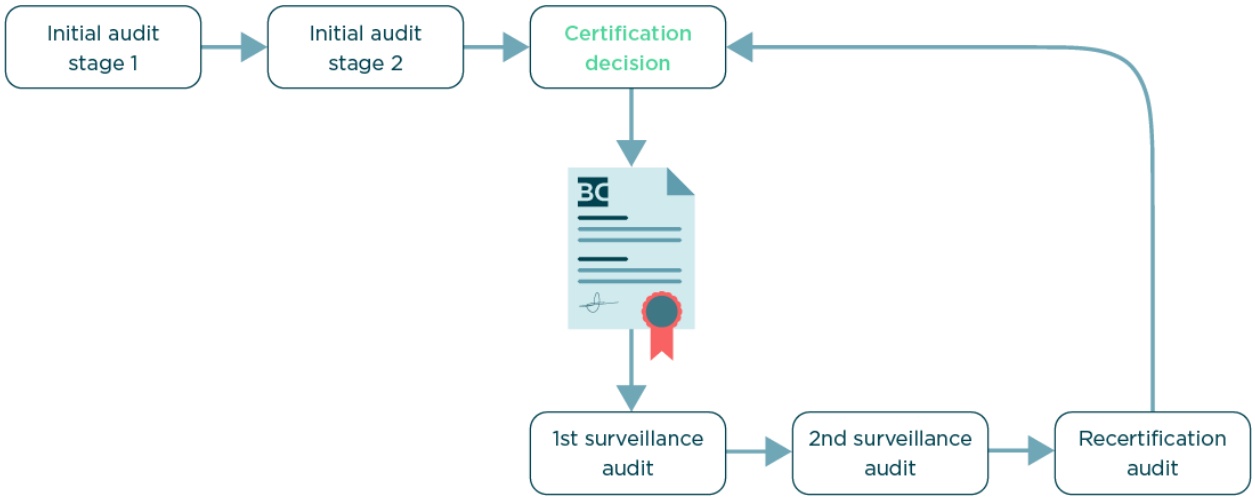
In this chapter we will describe the entire certification process.

The certification process starts with an application for certification by the organisation. This application is used to draft an agreement. Upon receiving the confirmation of the agreement, Brand Compliance will schedule the audit days in consultation with the organisation. After that, both parties start their preparations and the initial audit is held on the scheduled dates.

The initial audit is divided in a stage one and stage two audit. A report is drafted after the stage 1 and stage 2 audit, which is then reviewed by an independent certification committee. The committee decides whether or not to issue the certificate to the organisation.

During each stage the (Lead) Auditor may identify nonconformities and/or defects. These must be addressed before certification is possible. See paragraph 2.10.

The certification cycle will start after the initial audit decision. This cycle is reflected in the image below.



To retain the certificate, each certified organisation must have the subsequent audit in the cycle conducted annually (within 12 months after the closing meeting of the previous audit). The cycle consists of two surveillance audits, after which a recertification audit will be conducted at the end of the three-year period. Once the new certification decision has been made, a new cycle will start.
Brand Compliance will inform the organisation about the upcoming audits in the course of the process. The organisation has the option to make an appointment for the next audit in an earlier stage.

2.1 Application for certification

The organisation's application is recorded on the application form. The recorded information is based on the data provided by the organisation. This information allows us to estimate the required time for the audits and certification.

For each organisation, Brand Compliance will determine how much time is needed to conduct a full and effective audit in accordance with the BC 5701:2024 Certification Scheme. The calculation of the time to be allocated is based on the table in the Certification Scheme, and factors that may affect the time required for certification. Planning, preparation and reporting are also part of the total time allocated. Based on this, Brand Compliance will make a proposal to the organisation.

2.2 Certification agreement

Brand Compliance will send the organisation a proposal including an agreement. The organisation may accept the offer by returning it signed or by sending Brand Compliance an e-mail with their confirmation.

2.3 Scheduling

Upon receiving the acceptance of the agreement, Brand Compliance will plan an appropriate date for the execution of the audit in consultation with the organisation. In consultation, either the first and second audit will be planned immediately or the second stage will be planned after successful completion of the first stage.

Brand Compliance's policy is to perform their services using their own staff. Outsourcing of audit or inspection activities does not occur. However, we do occasionally hire extra capacity by using external staff, i.e. a technical expert. Brand Compliance regards their hired staff as their own staff and such staff also signs a confidentiality statement and a statement of independence.

The contract Brand Compliance enters into with hired staff, includes the same obligation of secrecy and rules of conduct with regard to confidential business data of the organisations as those applicable to their own staff.

Hired staff will present themselves as Brand Compliance staff, but do not play a role in executive services. They will not take the final certification decision. The statement of independence includes the obligation for hired staff to report if their independence may be affected in their assignments for Brand Compliance.

2.4 Preparation

In order for the audits to proceed smoothly, preparation by both Brand Compliance and the organisation is required.

2.4.1 Preparation by Brand Compliance

In order to carry out the audit correctly, the (Lead) Auditor will have to gain in-depth knowledge of the organisation. To this end, the (Lead) Auditor may request specific documents from the organisation. The organisation will be informed of this in a timely manner by the (Lead) Auditor. Additionally, the (Lead) Auditor will draw up a full audit programme. Based on this, an audit plan is drawn up which is shared with the organisation prior to the audit. It specifies which employees will be interviewed and when, and which parts of the organisation will be audited.

2.4.2 Preparation by the organisation

The organisation must have carried out at least one management review of the process to be certified and at least one internal audit covering the Target of evaluation prior to the audit. In addition, the implemented requirements must have been operational for at least three months to determine their correct functioning.

2.5 Initial audit

Certification starts with an initial audit. This audit consists of two parts: stage 1 and a stage 2.
The starting point of the audit is to gather evidence that the processing and protection of personal data takes place in accordance with the GDPR and the organisation is in control of this processing of personal data in accordance with the requirements of the GDPR Certification Standard and Criteria BC 5701:2024.

2.5.1 Co-operation by the organisation

A successful audit requires sufficient information to establish that the processing and protection of personal data has been designed, implemented and carried out in accordance with the requirements of GDPR Certification Standard and Criteria BC 5701:2024.

The Accreditation Council will assess from time to time whether Brand Compliance continues to meet the requirements of ISO 17065. Part of this assessment may include attending activities at a client's site. In this case, the organisation will be informed in a timely manner.

2.5.2 Initial audit - stage 1

During stage 1, the extent to which the processing in its set-up meets the requirements of the GDPR, the requirements from other laws and Regulations and the requirements of other stakeholders, and the extent to which the management system developed by the organisation regarding the processing and protection of personal data in its set-up meets the requirements of the GDPR Certification Standard and Criteria BC 5701:2024.

2.5.2.1 Opening meeting

During the opening meeting, the organisation’s management will receive information about the assessment process, including the audit planning, certification criteria and assessment method. During this opening meeting, we will also discuss how to act when changes in, for example, the target of evaluation or the audit time are necessary. Brand Compliance has drawn up guidelines for this and will determine the actions in consultation with the organisation.

2.5.2.2 Audit - Stage 1

A stage 1 audit will include at least the following:

- ✓ the organisation's documented information for the processing activities and the management system;
- ✓ agreements with processing relations;
- ✓ assess the status of the organisation and their understanding of the requirements of GDPR Certification Standard and Criteria BC 5701:2024, in particular with regard to identifying the main

performance of the data processing and data protection and the management system of significant aspects, processes, objectives and execution;
- ✓ the specific circumstances of the organisation's site and interviews with staff to determine its readiness for stage 2;
- ✓ obtain the necessary information regarding the target of evaluation, including:
  - the business location(s) of the organisation;
  - determining the target of evaluation;
  - the definition of the scope of the target of evaluation;
  - processes and equipment used;
  - level of implemented controls;
  - requirements from applicable laws and Regulations and stakeholder requirements;
- ✓ assess the allocation of resources for stage 2 and agree with the organisation on the details of stage 2, including the information needed to perform the required sampling;
- ✓ plan stage 2 by gaining sufficient insight into the organisation's processing and protection activities and the organisation's management system at the relevant business location, in relation to GDPR Certification Standard and Criteria BC 5701:2024 and other normative documents;
- ✓ assess whether the internal audits and the management reviews are planned and executed and whether the degree of implementation of the management system indicates that the organisation is ready for stage 2.

2.5.3 Initial audit - stage 2

The purpose of stage 2 is to gather evidence that the processing and protection of personal data and data subjects' rights are carried out as designed, the management system functions as designed and the organisation is in control with respect to changes affecting the target of evaluation.

2.5.3.1 Audit - stage 2

A stage 2 audit will include at least the following:
- ✓ information and proof of compliance with all requirements GDPR Certification Standard and Criteria BC 5701:2024;
- ✓ performance monitoring, measurement, reporting and assessment in relation to the main performance targets and programme targets (in accordance with the expectations in the GDPR Certification Standard and Criteria BC 5701:2024);
- ✓ the ability of the organisation's management system and the performance of that system in meeting the requirements of applicable laws and Regulations and contractual requirements;
- ✓ operational control of the organisation's processes;
- ✓ internal audits/assessments and management review;
- ✓ management responsibility for the organisation's policies.

2.5.3.2 Closing meeting

Any nonconformities and defects observed will be discussed and reported during the closing meeting. In conjunction with the organisation's management, the (Lead) Auditor will give an overview of the findings, classify any nonconformities and defects and discuss the corresponding settlement. The (Lead) Auditor will also indicate whether the organisation is nominated for certification. Based on what is

found during stage 1, Brand Compliance reserves the right to retake stage 1 and/or to postpone or cancel stage 2.

2.6 Reporting

After the stage one and stage two audits, the (Lead) Auditor will prepare a report with the findings. This report covers all aspects of the standard, including the way they are implemented by the organization.

2.7 Certification decision

After completion of the full initial audit (stage one and two), an independent certification committee will advise whether the certificate may be issued, based on the report. The certification decision is then made. In case of a positive result Brand Compliance will issue a certificate to the organisation, with which the organisation can demonstrate that its organization meets the requirements of the standard.

2.8 Surveillance audits

Surveillance audits will take place annually, twice in each certification cycle. The purpose of this is to establish ongoing compliance with the requirements of the GDPR Certification Standard and Criteria BC 5701:2024, and thus the lawfulness of processing and the adequacy of personal data protection.

Nonconformities or defects may be identified during a surveillance audit. This is explained in paragraph 2.10. Such nonconformities must be resolved within the term set, so that the certification may be continued.

2.9 Recertification

Recertification must be completed three years after the initial audit. The purpose of a recertification is to confirm the continuity and effectiveness of the processing procedure, the continued relevance and applicability of the target of evaluation. This refers to the operation during the certified period.

Recertification will be carried out approximately 3 months before the expiry date of the certificate. Any nonconformities or defects observed must be assessed by the audit team as resolved before the end of the certificate in order to be able to guarantee continuity of the certificate.

2.10 Nonconformities and defects

During the audits, different nonconformities and/or defects may be identified. Nonconformities and/or defects are issues within the set-up and/or implementation of the requirements that have to be resolved, before certification is possible. Nonconformities relate to the organisation's ability to meet the requirements of the standard. Defects relate to (not) meeting a legal requirement.

Nonconformities are divided into two categories:

1) Major nonconformities (Category A): non-fulfilment of a requirement that affects the capability of the management system to achieve the intended results. Nonconformities could be classified as major in the following circumstances:
    - if there is significant doubt that affective process control is in place, or that products or services will meet specified requirements;

- a number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity.

2) Minor nonconformities (Category B): non-fulfilment of a requirement that does not affect the capability of the management system to achieve the intended results.

Defects are also divided into two categories:

Defect A: Any action or omission in conflict with the GDPR and/or applicable laws and/or Regulations and/or requirements of interested parties, which directly affects the rights and freedoms of data subjects.
Defect B: Any action or omission in conflict with the GDPR and/or applicable laws and/or Regulations and/or requirements of interested parties, which does not directly affect the rights and freedoms of the data subjects.

The following may also be noted:

- Opportunity for improvement: indicates inefficiency and area for improvement. This follows indirectly from the certification requirements and must be considered.
- Area of concern (AoC); weak point that could be classified as a nonconformity during stage 2.

2.11 Term to resolve nonconformities

In case of nonconformities, depending on the category of the nonconformity, a term is set by the auditor within which the nonconformity must be resolved or a plan of action submitted.

If in the case of an initial audit Brand Compliance is unable to verify the implementation of corrections and corrective actions for a major nonconformity within 6 months of the last day of Stage 2, Brand Compliance must conduct Stage 2 again before recommending certification.

For a recertification the validity period of the certificate is leading. If the settlement of nonconformities does not take place within the validity period of the current certificate, this must then be done within 5 months (calculated from the certificate's validity date). If this is the case, a new certificate may be issued. The starting date on the certificate then equals the date of the recertification decision and the expiry date is based on the previous certification cycle. If the 5-month deadline is not met, a new initial audit (at least stage 2) must be carried out to maintain a certificate.

2.12 Term to resolve defects

All defects found during the inspection must be resolved before certification can proceed. The maximum time limit for resolving defects depends on the defect category:

A defect within category A must be resolved within a period of 0 to 4 weeks, at the discretion of the Lead Auditor, depending on the risk to those involved. If the defect cannot be rectified or resolved within the period set by the Lead Auditor, the processing in question must be discontinued or excluded from the target of evaluation.

A defect within defect category B should be resolved within a period of 0 to 3 months, depending on the severity of the activity. This is determined by the Lead Auditor. Different requirements may apply in specific situations; these are included in the audit methodology.

2.13 Corrective actions

Corrective actions may be taken to resolve the nonconformities and defects. Two categories of corrective actions are distinguished:

I Corrective actions that merely change the documented management system. In this case, the nonconformity report will be closed by submitting written proof, and verification on-site is not necessary;

II Corrective actions that contain changes that require on-site verification. In that case Brand Compliance will arrange and perform an additional audit.

2.14 Settlement

The reply to the identified nonconformities and defects by the organisation shall always include the following parts:

- ✓ cause analysis;
- ✓ correction;
- ✓ corrective action.

The organisation may provide this information in hard copy or electronically. The relevant auditor will ensure that the elements above are included in the reaction for each nonconformity and defect identified.

In case of major nonconformities (category A) corrections and corrective actions will be examined within 5 months after the last audit day.

3 Use of certificates and logos

Specific rules apply regarding the use of certificates and logos. When the certification audit has been successfully completed, the organisation will be entitled to a certificate and the right to use the certified logos corresponding to GDPR Certification Standard and Criteria BC 5701:2024. From that moment on, the organisation may use the logos for their corporate identity or marketing purposes, for example.

The certificate holder shall ensure that no confusion is possible regarding the target of evaluation and the mark issued by Brand Compliance. If Brand Compliance finds incorrect or unjustified use of the mark, Brand Compliance will ask the organisation to rectify this.

Certificates, seals and marks may only be used in accordance with Articles 42 and 43 of the GDPR.

3.1 Certificate

After a successful conclusion of the certification audit, Brand Compliance will provide a certificate, stating which standard(s) was/were tested as well as the assessed business activities and the period of validity.

In accordance with the requirements of the accreditation standards, Brand Compliance will keep records of organisations to which certificates have been issued, the associated targets of evaluation and the role from which the organisations carry out the certified processing. This register is available to third parties. Information outside the accreditation standard will only be provided to third parties with the written consent of the organisation.

3.1.2 Visibility of the certificate

In the case of certification under accreditation, the certificate will include the logo of the relevant accrediting organisation. The organisation has the right to exhibit this certificate at their business location or show it to individual stakeholders. For this purpose the certification mark may be used, see paragraph 3.2.

3.1.3 Termination of agreement

The organisation may terminate the Agreement in accordance with the conditions set out in the Agreement. Notice must be given in writing. Brand Compliance will then send a written confirmation. The organisation shall destroy all certificates in their possession as of the termination date. Also remove any logos, marks or expressions, for example on a website, to avoid any unauthorised use.

If logos, marks or expressions are not removed in a timely manner, the penalty clause, as described in this document under paragraph 3.4, will come into effect. Brand Compliance reserves the right to inspect on-site, unannounced, for unauthorised use after termination of the Agreement.

3.2 Certified Logo's

During the certificate's period of validity, the organisation also has the right to use Brand Compliance logos for promotional purposes. Brand Compliance has deposited their logos at the Benelux Trademarks Office under no. 1402095. Brand Compliance will provide the organisation with a set of original logos to this end. Brand Compliance will monitor the correct use during surveillance audits and recertification. Specific requirements apply to their use, you can read about it in paragraph 3.2.1.

3.2.1 Use of certified logos

The logo may be used on correspondence, advertisements, promotional materials and electronic media, on walls, doors and windows and on exhibition stands, provided that the communication is not misleading and in accordance with the requirements of these Regulations. The logo may not be affixed to products.

The Brand Compliance logo is to be used as follows:

- ✓ either in black on a white background or in colour on a white background;
- ✓ if not otherwise possible, on a coloured background in white;
- ✓ the width should be at least 50mm;
- ✓ all numbers and letters in the mark must be legible;
- ✓ if the mark is enlarged, the space between the characters should be increased proportionally.

Example:
Brand Compliance certified mark, BC 5701

(25 * 79 mm)

If the organisation has any doubts about the use or wishes to deviate from the dimensions indicated above for the Brand Compliance Mark, please contact marketing@brandcompliance.com.

3.2.2 Certifications under accreditation

The certificate holder may use the RvA mark specifically provided to Brand Compliance; the Regulations for Use are available on the website of the RvA (www.rva.nl). The document is available under the name BR001 "Policy rule Accreditations".

Example of an RvA mark:

(25*25 mm) (25*25 mm)

3.3 Use of the name Brand Compliance

The organisation may use the name Brand Compliance for marketing purposes, including social media and email, in the context of communication about certification activities.

When using certificates, declarations of conformity and/or audit reports issued by Brand Compliance, the organisation will act in such a way that Brand Compliance's reputation and impartiality is not affected. All announcements will be arranged in such a way that no misleading impression is created with regard to the applicable target of evaluation or business location of the certification, or the applicable standards and requirements.

3.4 Unauthorised use

Certification marks, signs or logos may not be used for the following purposes:

- the organisation shall not give third parties the impression that Brand Compliance is responsible for the activities of the organisation;
- the organisation shall not affix marks that may be confused with the certification marks and/or other signage mentioned in the Certification Agreement;
- logos or marks may not be applied to test reports from laboratories, calibration or test reports or test certificates.

In case of unauthorised use of the certificate and/or certification logo(s) and/or marks, Brand Compliance will impose a penalty of 750 euros for each day that said breach continues.

4 Maintaining the certificate

During the certification period, Brand Compliance will remain responsible for the decision it has taken concerning the target of evaluation, including issuance, maintenance, renewal, expansion, limitation and withdrawal of the certificate.

To maintain the acquired certificate, the organisation, including all entities that full under the certification, should:

- always fulfil both the general certification requirements and the criteria adopted by the supervisory authorities or the European Data Protection Board (EDPB) following Articles 43.1.b and 42.5 GDPR;
- offer full transparency to the organisation's supervisory authority regarding the certification procedure, including all the confidential material, contractual or otherwise, relating to compliance with the data protection prescriptions under Articles 42.7 and 58.1.c GDPR;
- shall provide the certification body with all information and access to its processing activities as required to carry out the certification procedure following Article 42.6 GDPR;
- enable the certification body to announce the reasons for awarding or withdrawing the certification under Article 43.5 GDPR to the organisation's supervisory authority, as well as the information that the organisation's supervisory authority will have to submit to the EDPB so that the latter can include the certification mechanism in a public register following Article 42.8 GDPR;
- have rules for the required preventive measures for the investigation of complaints;
- inform the certification body of any breaches of the GDPR or the Member States' GDPR implementation act(s) that the relevant supervisory authority or authorities, legal authorities, or both have established, and that may impact the certification when they know of such a breach;
- always fulfil the certification requirements, including implementing appropriate changes when they are communicated by the certification body;
- always report data breaches related to the target of evaluation.

And in addition, the organisation should make all necessary arrangements for:

- the conduct of the audit, including provision for examining documentation and records, and access to the relevant equipment, location(s), area(s), personnel, and subcontractors;
- investigation of complaints;
- the participation of observers, if applicable;
- the organisation makes claims regarding certification consistent with the scope of certification;
- to not use the certification in such a manner as to bring the certification body into disrepute and does not make any statement regarding its certification that may be considered misleading or unauthorized;

- upon suspension, withdrawal or termination of certification all use over advertising material that contains any reference to the terminated certification must be discontinued;
- if copies of the certification documents are provided to others, these shall be reproduced in their entirety;
- in making reference to its certification in communication media, such as documents, websites or other forms of advertising, this will comply with the requirements of the certification body (see chapter 3);
- to comply with any requirements that are prescribed in these Certification Regulations relating to the use of marks and information related to the product/service/process;
- keeping a record of all complaints made known to them relating to compliance with the certification and making these records available to the certification when requested;
- taking appropriate action with respect to such complaint and any deficiencies found in processes that affect the compliance with the requirements for certification;
- documenting the actions taken;
- keeping this documentation for at least 5 years;
- informing the certification body, without delay, of any changes that may affect its ability to conform with the certification requirements.

Regardless of whether the organisation holds a certificate, the organisation shall always comply with its legal obligations, obligations arising from certification and other obligations that may be imposed on the processing and protection of personal data (e.g. other normative documents or technical obligations).

4.1 Interim changes

If the organisation changes its management system or process in a significant way during the certificate's period of validity, the organisation must notify Brand Compliance of such changes. Such changes include, for example, changes related to:

- the legal form, organisational form or ownership;
- organisation and management (e.g. key personnel in management positions, decision-making positions or at technical level);
- contact address and business locations;
- significant changes relating to the target of evaluation;
- the state of the technology with regard to data protection or the target of evaluation;
- personal data breach related to the object of certification.

Brand Compliance will review the changes in relation to the requirements of the standard. Major changes may lead to an audit in the short term. The receipt of a complaint about the organisation, may also result in an audit in the short term. Minor changes to the management system, process or documents will be reviewed by the auditor during the next regular audit.

4.1.1 Statutory certification activities

The organisation must notify Brand Compliance of any change that affects how the organisation meets the requirements of the GDPR Certification Standard and Criteria BC 5701:2024. Brand Compliance will

review the proposed changes and decide whether the amended assurance system still complies with the requirements, or whether a new assessment is necessary. Brand Compliance will inform the organisation of its decision. This notification contains the conclusions of the assessment and the reasoned assessment decision.

4.1.2 Changes of certification requirements

If the certification requirements change during the certification period, Brand Compliance will timely inform the organisation of this change and discuss possible actions for organisation to be able to meet the requirements of the standard.
If any changes in the processing and/or protection of personal data and/or the management system are to be implemented, Brand Compliance reserves the right to review such changes.

In case of changes regarding Brand Compliance's accreditations or if an accreditation is cancelled, Brand Compliance will timely inform the certificate holders.

5 Suspension, limitation and withdrawal of the certificate

In specific cases, Brand Compliance may decide to suspend the certification. The organisation will be notified if this occurs. In general, suspension will be considered if the organisation:

- ✓ does not take corrective actions within the stipulated period;
- ✓ has not been able to handle the determined nonconformities within the stipulated period.
- ✓ persistently or substantially fails to meet the certification requirements, including the requirements for the effectiveness of the management system;
- ✓ does not agree to surveillance or recertification audits being conducted at the required frequency;
- ✓ uses the certificate and/or logo(s) in an unauthorised way;
- ✓ does not fulfil its (financial) obligations towards Brand Compliance;
- ✓ causes to affect Brand Compliance's good name and/or business reputation;
- ✓ voluntary suspension request.

Brand Compliance shall do everything within its power to enable the organisation to take appropriate measures. Brand Compliance may perform an additional audit to verify the effectiveness of the measures taken.

5.1 Limitation of the target of evaluation

If the organisation fails to take corrective measures within the agreed period, the certificate may be withdrawn or the target of evaluation may be limited.

Brand Compliance will limit the target of evaluation to exclude the parts that do not meet the requirements, if the organisation does not consistently or substantially comply with the certification requirements for the relevant parts of the target of evaluation. Such a limitation must be in accordance with the requirements of the GDPR Certification Standard and Criteria BC 5701:2024.

In the event of a limitation of the target of evaluation stated on the certificate, at the request of the organisation or by observation of the auditor, communications shall be adjusted, for example a copy of the certificate on the company website, so as not to create the impression that the organisation is still certified for the activities concerned.

5.2 Maintaining the certificate

If at any time during the certification period of three years, the organisation does not wish to retain the certificate or considers they are not capable of doing so, Brand Compliance will withdraw the certificate after being notified.

In the event of suspension or withdrawal, the organisation shall immediately refrain from carrying the relevant certificate, certification mark or declaration and refrain from giving the impression, in whatever way, that it is still entitled to the certification concerned. The same applies in the event that the agreement is terminated by one of the parties.

5.3 Disclosure

Suspension, withdrawal and limitation of the scope of the certificate will be conducted by Brand Compliance and the organisation will be notified of this in writing. Brand Compliance will publish notice of suspension and withdrawal of the relevant certificate. Brand Compliance has no influence on the registration of issued, expired and possibly withdrawn certificates maintained by third parties on the Internet.

The documents and data provided by the organisation (including information carriers) may be inspected by a third party during an audit they conduct at Brand Compliance (for example the Accreditation Council or the Impartiality Committee).

5.4 Complaints, objections and appeal against withdrawal of the certificate/limitation of scope

If the organisation disagrees with Brand Compliance's decision to withdraw or suspend the certificate, the procedure as described in chapter 6 will be followed.

6 Complaints, objections and appeal

6.1 Complaints

If the organisation is not satisfied with the way in which Brand Compliance performed the audit, a complaint may be submitted by using the “Brand Compliance complaint form” published on our website.

6.2 Procedure

Complaints are handled according to our complaints procedure. A written confirmation of receipt will be sent to the submitter within 5 working days of receipt. The investigation of the complaint takes a maximum of 10 working days. The decision will be communicated to you in writing.

All complaints submitted, will be recorded. The Area Director will appoint a person responsible for handling the complaint. The owner of the complaint will ensure verification and reproducibility of the handling. The full procedure is published on the website of Brand Compliance.

Brand Compliance has the authority at all times to review a complaint with the organisation without disclosing the source of the complaint.

6.3 Objections and appeal

If the organisation wishes to appeal against a decision by Brand Compliance regarding:

- non-acceptance of an application for certification;
- not to recommend certification;
- suspension, withdrawal or cancellation of the certificate;
- objection by third parties against the issuance of a certificate.

such appeal must be filed within four weeks of the relevant fact. Appeals are processed in the same way as complaints. Submission, investigation and decisions regarding appeals shall not result in actions against the organisation.

7 Independence and objectivity

Brand Compliance is aware of the fact that it must adopt and maintain an impartial position while performing certification activities. For this reason, we have taken measures to prevent conflicts of interest.

As a result:

- Brand Compliance can provide training to clients for whom certification activities are carried out, providing general information that is also publicly available, but no company-specific training is provided;
- Brand Compliance cannot provide internal audits/reviews or other advisory services with regard to the management system to be certified, for clients for whom certification activities are performed;
- Brand Compliance takes an independent position with regard to the persons or bodies that do carry out internal audits/reviews or other advisory services at clients to be certified;
- Brand Compliance can identify points for improvement in the management system of customers for which certification activities are carried out, but cannot provide advice on the details of the measures to be taken;
- Brand Compliance cannot certify certification bodies or get certified itself;
- Brand Compliance's Impartiality Policy requires employees not to accept gifts from customers.