# GDPR Certification Standard and Criteria

BC 5701:2024

**Een officieel Europees gegevensbeschermingszegel**

Een whitepaper van

Brand Compliance

piims academy

# Colofon

Deze whitepaper is een uitgave van:

### *Tekst en redactie*

**Piims Academy BV**
Kernauteur BC 5701
www.piimsacademy.com

**Brand Compliance BV**
Certificerende instelling BC 5701
www.brandcompliance.com

### *Opmaak*

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

### *Druk*

**Drukwerkdeal**
Online drukkerij
www.drukwerkdeal.nl

# Inhoud

*De waarde van AVG-certificering..... 1*

*De opbouw van de BC 5701..... 4*

*Voor wie en wat geschikt..... 7*

*De inhoud van de BC 5701..... 8*

*De fase in het goedkeuringsproces..... 10*

*De BC 5701 voor iedere organisatie..... 11*

*Implementatie en certificering..... 12*

*De organisaties achter de BC 5701..... 14*

**Disclaimer**

Deze whitepaper heeft als doel belangstellenden een algemeen beeld te geven van de GDPR Certification Standard and Criteria BC 5701:2024. Omwille van de overzichtelijkheid schetsen wij soms een vereenvoudigde weergave van de werkelijkheid. Aan deze whitepaper kunnen daarom geen rechten worden ontleend.

# GDPR Certification Standard and Criteria

BC 5701:2024

## Een officieel Europees gegevensbeschermingszegel

Na jaren van ontwikkeling en een zeer uitgebreid goedkeuringsproces, konden we in oktober 2023 de goedkeuring vieren van de BC 5701 als nationaal certificeringsmechanisme voor de AVG. Een jaar later is de 2024-versie van de BC 5701 goedgekeurd als officieel Europees gegevensbeschermingszegel, zoals bedoeld in artikel 42, lid 5, AVG. De BC 5701 is daarmee de nieuwe standaard in aantoonbare AVG-compliance en kan worden toegepast in alle landen van de EER. Met deze whitepaper informeren wij u over de opzet, de achtergronden en de inhoud van de certificeringsstandaard. We geven een beeld van het goedkeuringsproces, leggen uit wat de goedkeuring inhoudt laten zien hoe u uw voordeel kunt doen met deze nieuwe standaard.

## De waarde van AVG-certificering

Voor dat we inzoomen op de ins en outs van de BC 5701, staan we even stil bij de waarde van een AVG-certificering. Met andere woorden: voor wie is het bedoeld en welke oplossing biedt het. Dit laten we zien vanuit twee perspectieven. Eerst kijken we naar de waarde voor de maatschappij en daarna naar de waarde voor de te certificeren organisatie.

### *De waarde voor de maatschappij*

Een van de belangrijke drijfveren achter AVG-wetgeving is het borgen van economische groei binnen de Europese Unie[1]. Onder invloed van de snelle technologische ontwikkelingen worden producten en diensten steeds complexer en steeds digitaler. Niet zelden kunnen zelfs professionals de producten en processen die ze inkopen niet meer volledig doorgronden. Dit betekent dat het belang van vertrouwen in het economisch verkeer steeds verder toeneemt. De belangrijkste vraag daarbij is: wat kan een goede basis zijn voor dit vertrouwen?

[1] Zie overweging 6 en 7 AVG.

De BC 5701 is ontwikkeld om op meerdere manieren bij te dragen aan het maatschappelijk vertrouwen. Allereerst geeft de BC 5701 het concept 'AVG-compliance' handen en voeten; het maakt AVG-compliance concreet. Zo helpt het organisaties bijvoorbeeld om de compliance-afspraken met verwerkingsverantwoordelijken en/of verwerkers echt betekenis en inhoud te geven. Ten tweede bevordert de BC 5701 de juiste implementatie van de AVG, wat weer direct bijdraagt aan een betere bescherming van persoonsgegevens. Ten derde biedt het BC 5701-beeldmerk alle stakeholders in één oogopslag de zekerheid van een integere en kwalitatief hoogwaardige verwerking van persoonsgegevens. Last but not least draagt de BC 5701 vanuit de implementatie-eisen bij aan een betere bescherming van- en een betere controle over de persoonsgegevens van de betrokkenen. Kortom: AVG-certificering maakt de 'vertrouwbaarheid' van de verwerking van persoonsgegevens aantoonbaar.

## *De waarde voor certificerende organisaties*

Elke organisatie die de bescherming van persoonsgegevens serieus neemt, loopt bij de uitwerking van de AVG tegen dezelfde soort problemen aan; ongeacht de grootte van de organisatie, de complexiteit van de verwerking of de AVG-rol van de organisatie. Deze problemen houden verband met de abstractie van de wet. Onderstaand lichten we drie veel voorkomende probleemthema's toe en geven wij aan hoe de BC 5701 organisaties helpt bij het oplossen ervan.

### De passendheid van de uitwerking

De passendheid van de uitwerking heeft te maken met de specifieke verwerkingscontext van de organisatie en de vraag wanneer de uitwerking goed (genoeg) is. De BC 5701 helpt organisaties bij de beantwoording van die vraag door precies aan te geven voor welke aspecten de organisatie maatregelen moet nemen en welke maatregelen dat moeten zijn. Ook helpt het de organisatie vast te stellen of de genomen maatregelen toereikend zijn.

### De AVG-compliance van externe partijen

Iedere organisatie maakt gebruik van verwerkers. De uitdaging daarbij is dat de organisatie geen operationele controle heeft over die activiteiten, maar daar wel verantwoordelijk voor is. Hoe stelt de organisatie consequent en toereikend de AVG-compliance van de verwerkers vast en hoe houdt de organisatie daarbij grip op de kosten? Want serieus beoordelen kost serieuze capaciteit.

De BC 5701 draagt op twee manieren bij aan een oplossing. Ten eerste geeft het de certificerende organisatie concrete handvatten voor het adequaat beoordelen van hun verwerkers. Daarnaast geeft certificering verwerkers de mogelijkheid om proactief hun AVG-compliance richting hun opdrachtgevers aan te tonen. Daarmee bieden verwerkers hun opdrachtgevers gemoedsrust, besparen ze hen veel tijd en verlagen ze de kosten van de samenwerking.

## Het aantonen van de eigen AVG-compliance

Wat misschien nog wel belangrijker is dan de wettelijke verplichting om de eigen AVG-compliance aan te tonen, is dat veel organisaties hun compliance aan willen tonen. Een compliance-verhaal moet daarbij, om geloofwaardig te zijn, wel aan drie voorwaarden voldoen:

1. de compliance is vastgesteld aan de hand van eenduidige criteria (toetsbaarheid);
2. de beoordeling is gedaan door een onafhankelijke partij (objectiviteit);
3. de beoordeling is van voldoende kwaliteit (betrouwbaarheid).

De BC 5701 is ontwikkeld om onbetwistbaar de AVG-compliance met betrekking tot een verwerking aan te kunnen tonen aan alle stakeholders van die verwerking.

### *De belangrijkste voordelen van AVG-certificering op een rij*

**Richting betrokkenen**

- Schept vertrouwen in een 'black-box-proces'
- Verbetert controle over eigen gegevens
- Verlaagt risico's van zaken doen

**Richting opdrachtgevers**

- Verlaagt 'cost of partnership'
- Bespaart controletijd
- Biedt gemoedsrust

**Richting de maatschappij**

- Draagt bij aan vertrouwen in de digitale economie
- Bevordert de juiste toepassing van de AVG

**Voor de eigen organisatie**

- Toont richting alle belanghebbenden de kwaliteit en integriteit van de verwerking(en) aan
- Ondersteunt actief het imago van een betrouwbare en vooruitstrevende organisatie
- Verbetert procesbeheersing
- Houdt het initiatief m.b.t. verantwoording (voor verwerkers)
- Verlaagt verwerkingsrisico's

## De opbouw van de BC 5701

In essentie is de BC 5701 opgebouwd uit drie blokken. Het eerste blok is de AVG zelf. Of beter gezegd: de eisen die vanuit de AVG gesteld worden. Voor een deel van die eisen, de eisen die betrekking hebben op de adequate bescherming van persoonsgegevens, wordt daarbij geleund op bestaande normen voor informatiebeveiliging (IB). Deze vormen het tweede bouwblok. Het derde en laatste bouwblok is een managementsysteem dat is toegevoegd om de toekomstige compliance te borgen. Samen vormen ze de drie bouwblokken van de BC 5701. Hieronder lichten we ze verder toe.


### *Bouwblok: AVG / GDPR*

De AVG schrijft voor dat certificering in het kader van de AVG gebaseerd moet zijn op ISO 17065. Deze eis heeft grote invloed op het certificeringsproces. ISO 17065 bevat namelijk eisen voor de certificering van producten, processen en diensten. AVG-certificering is dus een vorm van procescertificering. Dat is heel anders dan de bekende certificeringen zoals ISO 9001 (kwaliteit) en ISO 27001 (informatieveiligheid). Dat zijn namelijk managementsysteemcertificeringen. In de tabel op pagina 6 illustreren we het verschil tussen beide aan de hand van een voorbeeld. Onderstaand gaan we in op de betekenis voor het certificeringproces.

Dat de BC 5701 in de basis een vorm van procescertificering is, maakt dat een drietal aspecten wezenlijk anders zijn dan men op basis van de ervaring met managementsysteemcertificering zou verwachten. Ten eerste is de AVG (de bron van de certificeringseisen) erop gericht de belangen van de betrokkenen te beschermen. Dit maakt dat het perspectief van de BC 5701 ook automatisch dat van de betrokkenen is. Dus niet het belang van de organisatie staat voorop, maar het belang van de betrokkenen; het belang van de organisatie komt pas daarna. Ten tweede is de certificering gericht op verwerkingen en niet op de organisatie als geheel. Er moet dus duidelijk worden afgebakend wat er binnen en buiten de certificering valt. Ten derde zijn de certificatie-eisen specifieker en zijn de certificatieaudits diepgaander en strikter dan organisaties wellicht van certificeringen gewend zijn. Zo zal bijvoorbeeld van alle of praktisch alle verwerkers worden beoordeeld of de geschiktheid van de verwerker is vastgesteld; of alle verwerkings- en beschermingseisen juist zijn overeengekomen; of de naleving van de overeenkomst consequent en toereikend wordt gecontroleerd en of bij afwijkingen de passende maatregelen worden genomen. Met andere woorden: de certificeringsaudit is erop gericht om met een grote mate van zekerheid vast te stellen dat alle aspecten van de AVG op continue basis juist worden uitgevoerd en de kwaliteit daarvan is geborgd.

## *Bouwblok: IB-standaard (Informatiebeveiliging)*

De AVG kent (onder meer) het beginsel van “integriteit en vertrouwelijkheid”. Dit verplicht organisaties om passende technische en organisatorische maatregelen te nemen ter bescherming van de persoonsgegevens. Dat is het domein van informatiebeveiliging en daarbinnen bestaan al meerdere best practices die zich in de praktijk hebben bewezen. Daarom is voor de BC 5701 besloten om het wiel niet opnieuw uit te vinden, maar aan te sluiten bij erkende normen voor informatiebeveiliging. Voor organisaties die zich willen laten certificeren betekent dit, dat zij ook moeten voldoen aan een passende standaard voor informatiebeveiliging.

De IB-standaard moet vervolgens door de organisatie worden aangesloten op de BC 5701. De nadruk daarbij ligt op het eerder beschreven verschil in perspectief. Normen voor informatiebeveiliging zijn gericht op het beschermen van de belangen van de organisatie. AVG-certificering richt zich op de belangen van de betrokkenen. Aansluiting betekent dat de organisatie moet aantonen dat de beschermingsmaatregelen geschikt zijn om de risico’s voor de betrokkenen te vermijden of toereikend te verlagen.

## *Bouwblok: Managementsysteem*

Zoals eerder beschreven is AVG-certificering in de basis een procescertificering. Het doel is te toetsen of een verwerking van persoonsgegevens aan de eisen van de AVG voldoet. Onze ervaring heeft geleerd dat een dergelijke procesfocus niet tegemoetkomt aan de wensen van alle stakeholders. Een belangrijke reden voor organisaties om te willen certificeren is juist het wekken van vertrouwen bij hun stakeholders. Om dit vertrouwen te verkrijgen moet het certificaat niet alleen iets zeggen over de juiste verwerking en bescherming voorafgaand aan én ten tijde van het auditeren (historische perspectief), het moet ook iets zeggen over het vermogen van de organisatie om aan de verordening te blijven voldoen (toekomstperspectief). Daarnaast stelt artikel 42 lid 7 de eis dat de organisatie moet borgen dat zij bij voortduring aan de eisen van de AVG kan voldoen. Voor beide is het derde bouwblok toegevoegd: het managementsysteem. Het managementsysteem borgt dat de organisatie de continue veranderingen binnen en buiten de organisatie in overeenstemming met de AVG blijft implementeren.

***Procescertificering versus managementsysteemcertificering***

| *Onderwerp* | *Procescertificering* | *Managementsysteemcertificering* |
|---|---|---|
| De norm-eis | De organisatie moet ieder rechtmatig verzoek van betrokkenen aantoonbaar binnen één maand afhandelen. | De organisatie moet een proces en procedure opzetten voor het tijdig afhandelen van rechtmatige verzoeken van betrokkenen. |
| Kenmerken van de norm-eis | ▪ Heeft direct betrekking op de verzoeken van betrokkenen;<br>▪ is specifiek (extern gedefinieerd). | ▪ Heeft betrekking op het afhandelen/management van verzoeken van betrokkenen (is indirect);<br>▪ is algemeen (is afhankelijk van de 'tijdigheid' die de organisatie zelf bepaalt). |
| Audit | Met een bepaalde mate van zekerheid vaststellen dat alle verzoeken conform de eis zijn afgehandeld.<br><br>**Basis:** statistisch onderbouwde steekproef. | Vaststellen dat de procedure in staat is de doelen van de organisatie te behalen en dat de procedure overeenkomstig de opzet wordt uitvoert.<br><br>**Basis:** deelwaarnemingen. |
| Betekenis van conformiteit | De organisatie heeft alle rechtmatige verzoeken van betrokkenen binnen één maand afgehandeld.<br><br>*Dit is een uitspraak over de kwaliteit van het proces (output).* | De organisatie beheerst de tijdige afhandeling van verzoeken van betrokkenen.<br><br>*Dit is een uitspraak over de proces-beheersing door de organisatie (input).* |

Een vereenvoudigd voorbeeld van het verschil tussen procescertificering en managementsysteemcertificering voor het tijdig afhandelen van rechten van betrokkenen.

## Voor wie en wat geschikt

Natuurlijk kan de BC 5701 in ieder land worden gebruikt, maar de goedkeuring van de BC 5701 heeft betrekking op de landen van de EER. Oftewel, voor organisaties die in de EER zijn gevestigd. Daarbinnen kan de BC 5701 worden toegepast op elke verwerking van persoonsgegevens, ongeacht de branche waarbinnen dat gebeurt.
De essentie is dat:

1. de certificering betrekking heeft op een (cluster van) verwerkingen(en);
2. de organisatie verwerkingsverantwoordelijke of verwerker is ten aanzien van die verwerking(en).

De certificering heeft dus altijd betrekking op één of meer verwerkingen die vanuit een bepaalde AVG-rol worden uitgevoerd. Het is dus niet mogelijk om met de BC 5701 een product te certificeren. Neem bijvoorbeeld een slimme koelkast. De koelkast zelf kan niet gecertificeerd worden, maar de verwerking van persoonsgegevens die als service bij deze koelkast worden aangeboden kan wél worden gecertificeerd.

### *Het object van certificering*

Centraal binnen een certificeringstraject staat de verzameling aan verwerkingen die de organisatie wil certificeren. Binnen de BC 5701 heet deze verzameling het 'object van certificering'. Bij het bepalen hiervan is het belangrijk om het doel en de doelgroep van deze certificering voor ogen te houden. Het gaat immers om het creëren van vertrouwen bij de betrokkenen en/of opdrachtgevers. Het object van certificering moet daarom betekenisvol zijn voor die doelgroep. Dit betekent dat de certificering alle verwerkingen moet omvatten die horen bij het verwerkingsdoel van de doelgroep. Alleen dan krijgt de certificering voor hen waarde.
Het afbakenen en vaststellen van het object van certificering vormt dan ook het logische startpunt voor ieder implementatietraject van de BC 5701.

### *Het toepassingsgebied van de certificering*

Het object van certificering bepaalt welke verwerkingen gecertificeerd worden. Het toepassingsgebied beschrijft vervolgens alle aspecten van de organisatie die van invloed zijn op het object van certificering. Binnen de certificering moet geborgd worden dat ook deze aspecten in lijn met de AVG worden uitgevoerd. Denk bijvoorbeeld aan het ontwikkelen of wijzigen van de verwerkingen, de infrastructuur om de verwerking uit te voeren, het beleid dat kaders stelt ten aanzien van de verwerking, de medewerkers die bij de verschillende fasen van de verwerking betrokken zijn, et cetera. Dus hoewel de certificering gefocust is op een (set van) verwerking(en), raakt het certificeringsproces veel meer aspecten van de organisatie.

# De inhoud van de BC 5701

In dit hoofdstuk geven we u een overzicht van wat u in de BC 5701 aantreft.  De standaard kent 10 hoofdstukken. We lichten ze onderstaand kort toe.

## *Inleidende hoofdstukken*

De BC 5701 begint met 4 inleidende hoofdstukken; daarin staan nog geen uitvoeringseisen.

### Inleiding

De inleiding beschrijft de opzet van de norm. Er wordt uitgelegd hoe u de BC 5701 moet lezen.

### 1 - Onderwerp

Geeft een korte beschrijving van het onderwerp van de BC 5701. Het heeft geen operationele betekenis.

### 2 - Normatieve verwijzingen

Een kort maar belangrijk hoofdstuk. Hierin wordt beschreven welke wet- en regelgeving naast de AVG en de BC 5701 in ogenschouw moet worden genomen om voor certificatie in aanmerking te komen.

### 3 - Definities

Zoals de titel doet vermoeden bevat dit hoofdstuk de definities van de gebruikte termen en de betekenis van de gebruikte afkortingen en symbolen.

## *Hoofstukken met uitvoeringseisen*

Hoofdstuk 4 t/m 9 bevatten de maatregelen die organisaties moeten implementeren om aanspraak te kunnen maken op een certificaat. Binnen de hoofdstukken worden de onderwerpen steeds op dezelfde wijze uitgewerkt. Eerst een omschrijving van de (AVG) context, gevolgd door een te bereiken doelstelling. De doelstelling wordt vervolgens uitgewerkt in implementatie-eisen die leiden tot het bereiken van de doelstellig. Iedere paragraaf wordt afgesloten met de van toepassing zijnde artikelen en overwegingen van de AVG.

Per doelstelling en implementatie-eis is aangegeven of deze van toepassing is op verwerkingsverantwoordelijken, op verwerkers of op beide.

### 4 - Context van de verwerkingen

In dit eerste hoofdstuk met uitvoeringseisen wordt de organisatie gevraagd de interne en externe context van de verwerking te beschrijven. Daarnaast worden in dit hoofdstuk alle externe en interne eisen vastgesteld en vertaald naar eisen voor de verwerking. Tenslotte behandelt dit hoofdstuk de noodzakelijke afbakening van de certificering.

## 5 - Organisatie van de gegevensbescherming

In hoofdstuk 5 worden alle aspecten behandeld die op het niveau van de organisatie geregeld moeten worden; in plaats van op het niveau van de verwerking(en). Denk hierbij aan de betrokkenheid van de directie, beleid m.b.t. de bescherming van persoonsgegevens, de eisen m.b.t. de functionaris voor gegevensbescherming en het register van verwerkingsactiviteiten.

## 6 - Uitgangspunten van de verwerking

Hoofdstuk 6 richt zich op de opzet van de verwerking. Het gaat daarbij om het in kaart brengen van de verwerking, het uitwerken van de beginselen van de AVG en het uitwerken van de verwerkingsketen.

## 7 – Technische en organisatorische bescherming

Nadat de opzet van de verwerkingen is uitgewerkt, behandelt hoofdstuk 7 de aspecten die ondersteunend zijn aan de verwerking en bescherming van persoonsgegevens. Het bevat de eisen m.b.t. de eerder beschreven informatiebeveiligingsnorm, gaat in op het risicomanagement vanuit het perspectief van de betrokkenen, gegevensbescherming door ontwerp en door standaardinstelling en behandelt aspecten die ten aanzien van het betrokken personeel geregeld moeten worden.

## 8 – Operationele uitvoering

In dit voorlaatste hoofdstuk zijn alle eisen samengebracht die gaan spelen zodra de verwerking operationeel wordt. Onderwerpen die hier aan de orde komen zijn onder meer: de rechten van de betrokkenen, omgang met verwerkers, doorgifte van persoonsgegevens, inbreuken en het monitoren van veranderingen in de context van de verwerking.

## 9 - Managementsysteem

Hoofdstuk 9 tenslotte beschrijft het managementsysteem dat de organisatie moet implementeren. Het managementsysteem is er enerzijds op gericht om voortdurend de kwaliteit van de gegevensverwerking te monitoren en verbeteren. Anderzijds borgt het dat de organisatie veranderingen met betrekking tot de verwerking in overeenstemming met de AVG implementeert.

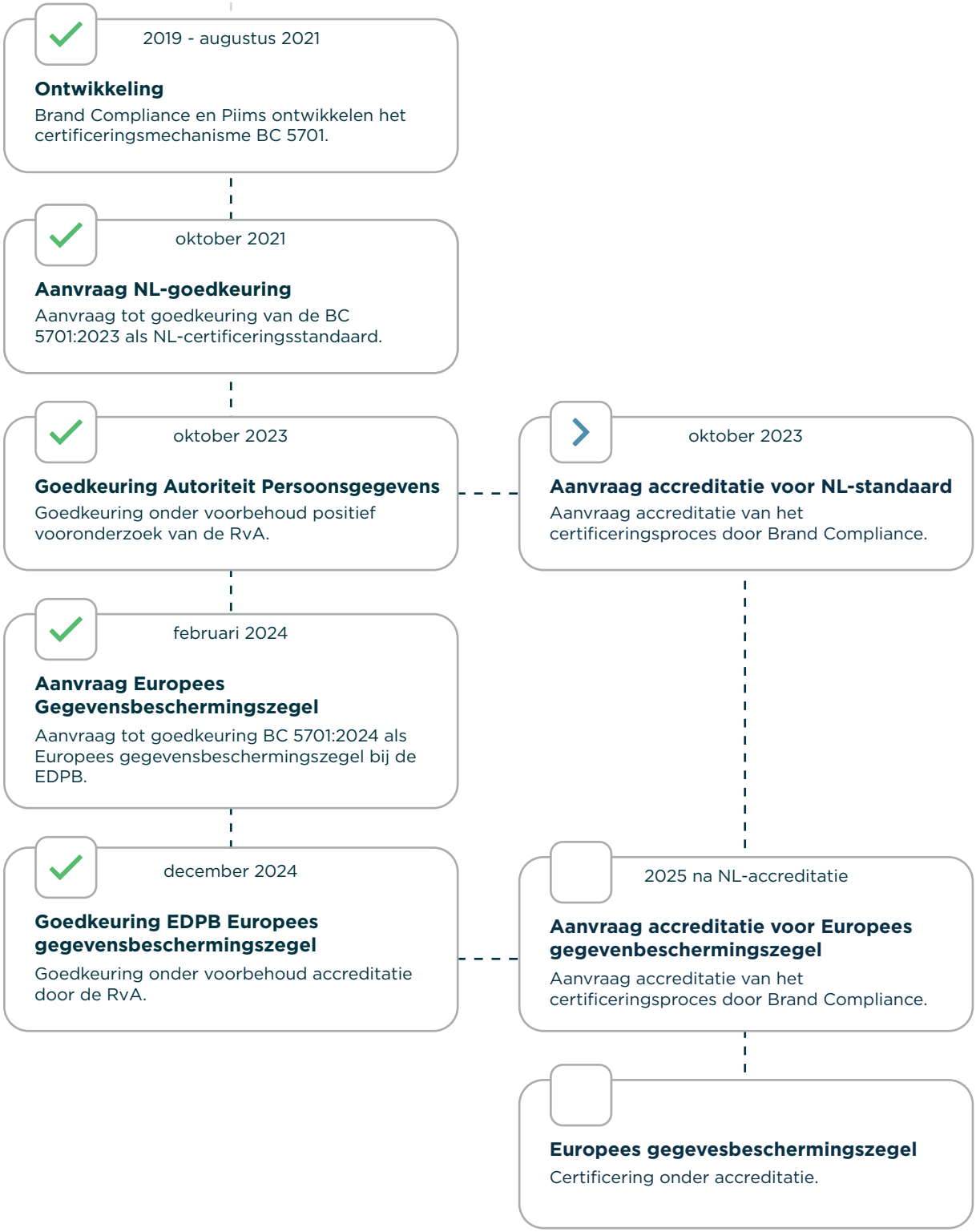
## *Bijlagen*

Tot slot zijn als bijlage een drietal informatieve overzichten opgenomen om organisaties te helpen bij de toepassing van de certificatiestandaard.

1. Overzicht van documentatievereisten
2. Kruisverwijzing AVG naar certificatiestandaard
3. Relevante richtlijnen EDPB

## Het goedkeuringsproces van de BC 5701

In december 2024, na een uitgebreid internationaal beoordelingsproces, heeft de European Data Protection Board (EDPB) GDPR Certification Standard and Criteria BC 5701:2024 goedgekeurd als Europees gegevensbeschermingszegel. Dit betekent dat alle toezichthouders van Europa van mening zijn dat toepassing van de BC 5701 leidt tot een aantoonbaar passende uitwerking van de AVG. Onderstaand schetsen we een beeld van het verloop van het goedkeuringsproces; de toekomstige data zijn verwachtingen.



## De BC 5701, voor iedere organisatie

Iedere organisatie die persoonsgegevens verwerkt kan met BC 5701 aan de slag. De standaard kan daarbij op twee manieren worden ingezet:

1. als (vrijblijvend) hulpmiddel bij het inrichten van de AVG-compliance, of
2. als leidraad bij het voorbereiden op een certificering.

### *Voorwaarde voor succesvolle certificering*

Wanneer u met het lezen van deze whitepaper tot hier bent gekomen, dan overweegt u wellicht om het certificaat te behalen. In dat geval willen wij u wijzen op nog een belangrijk aspect van AVG-certificering. Dat is de plaats binnen de organisatie waar u de AVG-compliance borgt. Benader de bescherming van persoonsgegevens als een kwaliteitsaspect van de reguliere operatie en niet als verantwoordelijkheid van het ondersteunend personeel. Het borgen van de AVG-compliance vanuit de reguliere werkprocessen zorgt ervoor dat dit altijd een punt van aandacht is en niet alleen wanneer het ondersteunend personeel daarop wijst. Het zorgt er ook voor dat zelfs de certificerings-audit geen verrassingen boven water haalt.

### *Nu is het moment om de slag te slaan*

Zoals gezegd kunnen we niet precies aangeven hoe lang de laatste fase van het goedkeuringsproces, de accreditatie van Brand Compliance, precies gaat duren. Maar laat dat u er niet van weerhouden om nu al te starten met de implementatie. Voor een gemiddeld implementatietraject moet u namelijk rekenen op een doorlooptijd van zes tot twaalf maanden. Als u een van de eerste organisaties in Europa wilt zijn die GDPR-gecertificeerd is, begin dan nu met uw implementatie.

**Leidraad voor certificering**

De GDPR Certification Standard and Criteria BC 5701:2024 bevat de vereisten waaraan organisaties moeten voldoen om in aanmerking te komen voor certificering.

De standaard beslaat ruim 180 pagina's en is voor € 295,- excl. btw (in het Engels) te koop op www.brandcompliance.com.

# Implementatie en certificering

Wanneer u overweegt een certificaat te behalen dan wilt u natuurlijk weten wat dit traject voor uw organisatie betekent. In dit hoofdstuk schetsen wij de contouren van zo'n implementatietraject.

## *GAP-analyse*

Waarschijnlijk heeft uw organisatie al behoorlijk wat werk verricht op weg naar AVG-compliance. De vraag is, hoe ver uw organisatie van dat doel verwijderd is? Welke stappen moeten nog gezet worden om aantoonbaar aan de BC 5701 te voldoen en wat is daarvan de impact? Dit vraagt om een gap-analyse. Zo'n gap-analyse kan grofweg op drie manieren worden uitgevoerd:

1. zelf uitvoeren na het bestuderen van de norm;
2. zelf uitvoeren na een opleiding tot BC 5701 Lead Implementor;
3. uit laten voeren door Brand Compliance of een bekwame implementatie-professional.

De ervaring leert dat de impact van de BC 5701 makkelijk wordt onderschat. Zekerheid omtrent de uitgangspositie van uw organisatie krijgt u met optie twee en drie. U wilt er immers niet pas tijdens de certificatieaudit achter komen wat de implementatiecriteria van de BC 5701 echt betekenen voor uw organisatie. Dat leidt tot veel onnodig werk, onnodige kosten en een aanzienlijke vertraging van het certificatietraject.

## *Implementatie*

Afhankelijk van de complexiteit van de verwerkingscontext, de AVG-volwassenheid van de organisatie en de beschikbare resources, zal uw implementatie door de band genomen ergens tussen de zes en twaalf maanden in beslag nemen.

Om u optimaal voor te bereiden op het implementatietraject bieden wij een opleiding aan met betrekking tot de implementatie. Hierin leren de deelnemers de voor de organisatie kritische elementen van de BC 5701 te doorgronden en toe te passen. Meer informatie hierover vindt u in het volgende hoofdstuk.

## *Operationalisatie en interne audit*

Nadat de implementatie is afgerond moet de organisatie vaststellen dat alle geïmplementeerde technische en organisatorische maatregelen werken zoals beoogd. Dit is onderdeel van het managementsysteem. De vaststelling vindt plaats door middel van een interne audit, gevolgd door een directiebeoordeling. Alle technische en organisatorische maatregelen moeten ten minste drie maanden volledig operationeel zijn om een betekenisvolle certificatieaudit uit te kunnen voeren.

## *Certificatie*

De certificatieaudit wordt uitgevoerd door een multidisciplinair auditteam met daarin juridische expertise, technische expertise en organisatorische expertise. Afhankelijk van de verwerkingscontext van de organisatie kan het auditteam worden uitgebreid met ondersteunende specialisten. De juridisch auditor richt zich op het beoordelen van de aspecten van rechtmatigheid. De technisch auditor richt zich op aspecten van de verwerking en bescherming van persoonsgegevens. De lead auditor tenslotte richt zich op de organisatorische aspecten van de implementatie en coördineert de audit.

## *Continuering van het certificaat*

Na het succesvol doorlopen van het certificatieproces wordt het BC 5701-certificaat afgegeven. Met dit certificaat toont de organisatie aan dat:

- de betreffende verwerkingen van persoonsgegevens in overeenstemming met de AVG worden uitgevoerd en
- dat de organisatie veranderingen in overeenstemming met de AVG doorvoert.

Het BC 5701-certificaat is in principe drie jaar geldig. Gedurende deze drie jaar moet de organisatie blijven aantonen dat zij in overeenstemming met de eisen werkt. Dit wordt jaarlijks door Brand Compliance beoordeeld aan de hand van zogenaamde ‘controleaudits’. Ook de controleaudits worden uitgevoerd door een multidisciplinair auditteam. Tijdens de controleaudits wordt vastgesteld of de organisatie gedurende de afgelopen periode in overeenstemming met de certificeringseisen heeft gewerkt en of de organisatie op de juiste wijze heeft gereageerd op veranderingen met betrekking tot de gecertificeerde verwerkingen.

Een certificatiecyclus bestaat dus uit een initiële audit en twee controleaudits. Aan het einde van de driejaarstermijn kan de organisatie kiezen voor hercertificering, waarmee de cyclus opnieuw begint.

Het BC 5701-certificaat toont de kwaliteit en integriteit van uw gegevensverwerking aan richting alle belang-hebbenden.

## De organisaties achter de BC 5701

Het certificeringsmechanisme BC 5701 is een gezamenlijke ontwikkeling van Brand Compliance en Piims Academy. Hieronder lichten we kort toe bij wie u met welke vragen terecht kunt.

Brand Compliance

Brand Compliance is een certificerende instelling die onder accreditatie certificatieaudits uitvoert op het gebied van kwaliteit, informatieveiligheid en privacy. Met betrekking tot de BC 5701 is Brand Compliance de beheerder van het certificeringsmechanisme en tevens de certificerende instelling. Voor de volgende onderwerpen bent u bij Brand Compliance aan het juiste adres:

- gap-analyses met betrekking tot de BC 5701;
- pilot deelname;
- certificeringsaudits.

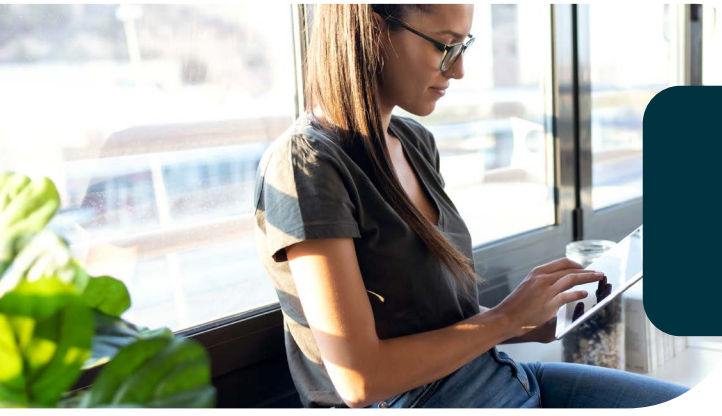
Meer informatie vindt u op: www.brandcompliance.com

Brand Compliance kan klanten waarvoor certificatieactiviteiten worden uitgevoerd, niet voorzien in interne audits/reviews of andere adviesdiensten met betrekking tot de te certificeren standaard.

piims academy

Piims Academy is kernauteur van de 'GDPR Certification Standard and Criteria BC 5701' en zet deze kennis in om mensen en organisaties te helpen bij het aantoonbaar passend uitwerken van de AVG. Piims Academy ontwikkelt en verzorgt de officiële BC 5701-opleidingen.

Meer informatie vindt u op: www.piimsacademy.com



Heeft u de ambitie om uw organisatie met de verwerking van persoonsgegevens op de kaart te zetten? Ga naar www.piimsacademy.com voor informatie over de BC 5701 Lead Implementor opleiding en verzeker uw succes.

Brand Compliance

www.brandcompliance.com
info@brandcompliance.com

piims academy

www.piimsacademy.com
info@piimsacademy.com