



AVG Certificeringsstandaard en -criteria

BC 5701:2023

de nieuwe standaard in AVG-compliance

een whitepaper van



Colofon

Deze whitepaper is een uitgave van:

Tekst en redactie

Piims Academy BV

Kernauteur BC 5701

www.piims.nl

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
Het goedkeuringsproces van de BC 5701	10
De BC 5701 (niet) 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 AVG-certificeringsnorm BC 5701:2023. Omwille van de overzichtelijkheid schetsen wij soms een vereenvoudigde weergave van de werkelijkheid. Aan deze whitepaper kunnen daarom geen rechten worden ontleend.



AVG Certificeringsstandaard en -criteria

BC 5701

De nieuwe standaard in AVG-compliance

Na jaren van ontwikkeling heeft de BC 5701 recent een belangrijke mijlpaal gehaald: goedkeuring door de Autoriteit Persoonsgegevens (AP). Dit betekent dat de AP heeft geoordeeld dat toepassing van de BC 5701 leidt tot een aantoonbaar passende uitwerking van de AVG. 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 organisaties hun voordeel kunnen 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 is van een AVG-certificering. Met andere woorden: voor wie is het bedoeld en welke oplossing biedt het. Dit laten we zien vanuit twee perspectieven, namelijk die van de maatschappij en die van de certificerende organisaties.

De waarde voor de maatschappij

De belangrijkste reden voor de AVG is het borgen van economische groei binnen de Europese Unie¹. Een absolute vereiste daarvoor is dat de maatschappij voldoende vertrouwen heeft én houdt in de economie. Want onder invloed van de snelle technologische ontwikkelingen worden producten en diensten steeds complexer. Vaak kunnen zelfs professionals de producten en processen die ze inkopen niet meer goed doorgronden. De belangrijkste vraag daarbij is: wat kan een goede basis zijn voor vertrouwen in het economisch verkeer? We weten dankzij de kredietcrisis immers allemaal wat de gevolgen kunnen zijn van ongegrond 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 aan hun opdrachtgevers te kunnen laten zien. 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

- Biedt vertrouwen in een 'black-box-proces'
- Verbetert control 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 bestaat de BC 5701 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 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 m.b.t. de certificering van producten, processen en diensten. Dat is heel anders dan 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 certificeringsproces.

Dat de BC 5701 in de basis een vorm van productcertificering 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 specifiek 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-norm (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 vorm van productcertificering. 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). Dus om aan de verwachtingen van alle stakeholders te voldoen, is het derde bouwblok, het managementsysteem, toegevoegd. Het managementsysteem borgt dat de organisatie de continue veranderingen binnen en buiten de organisatie in overeenstemming met de AVG blijft implementeren.

Product certificering versus managementsysteem certificering

Onderwerp	Productcertificering	Managementsysteemcertificering
De norm-eis	Een autoband van type X, moet bij een snelheid van Y km/u, Z liter water per seconde kunnen afvoeren.	De organisatie moet stelselmatig vaststellen dat de geproduceerde autobanden voldoen aan de door de organisatie gedefinieerde kwaliteitseisen.
Kenmerken van de norm-eis	▪ Heeft direct betrekking op de autoband (het product); ▪ is specifiek (extern gedefinieerd).	▪ Heeft betrekking op het management van het productieproces (is indirect); ▪ is algemeen (is afhankelijk van de normen die de organisatie zelf bepaalt).
Audit	Met een bepaalde mate van zekerheid en nauwkeurigheid vaststellen dat alle autobanden aan de gestelde eisen voldoen. Basis: statistisch onderbouwde steekproef.	Vaststellen dat de organisatie haar eigen beleid overeenkomstig de opzet uitvoert. Basis: deelwaarnemingen.
Betekenis van conformiteit	De organisatie maakt autobanden van een bepaalde kwaliteit.	De organisatie beheerst haar productieproces. (Er kan niet worden gezegd dat deze fabrikant goede autobanden maakt, want dat hangt af van de kwaliteitseisen die ze zichzelf opleggen en die ze zelf op ieder moment kunnen veranderen.)

Een vereenvoudigd voorbeeld van het verschil tussen productcertificering en managementsysteem certificering voor een fabrikant van autobanden.

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 Nederlandse markt. Oftewel, voor organisaties die in Nederland zijn gevestigd, met betrekking tot verwerkingen die in Nederland plaatsvinden en (ten minste) gericht zijn op betrokkenen die zich in Nederland bevinden. Daarbinnen kan de BC 5701 worden toegepast op elke verwerking van persoonsgegevens, ongeacht de branche waarbinnen dat gebeurt en ongeacht de verwerkingsrol die de organisatie vervult. De essentie is dat:

- 1 de certificering betrekking heeft op een (cluster van) verwerking(en)
- 2 de organisatie (gezamenlijk) 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 dus 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 de 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.

Hoofdstukken met uitvoeringseisen

In 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 implementatiecriteria die leiden tot het bereiken van de doelstelling. Ieder paragraaf wordt afgesloten met de van toepassing zijnde artikelen en overwegingen van de AVG.

Per doelstelling en implementatiecriterium 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 requirements 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 continu 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.

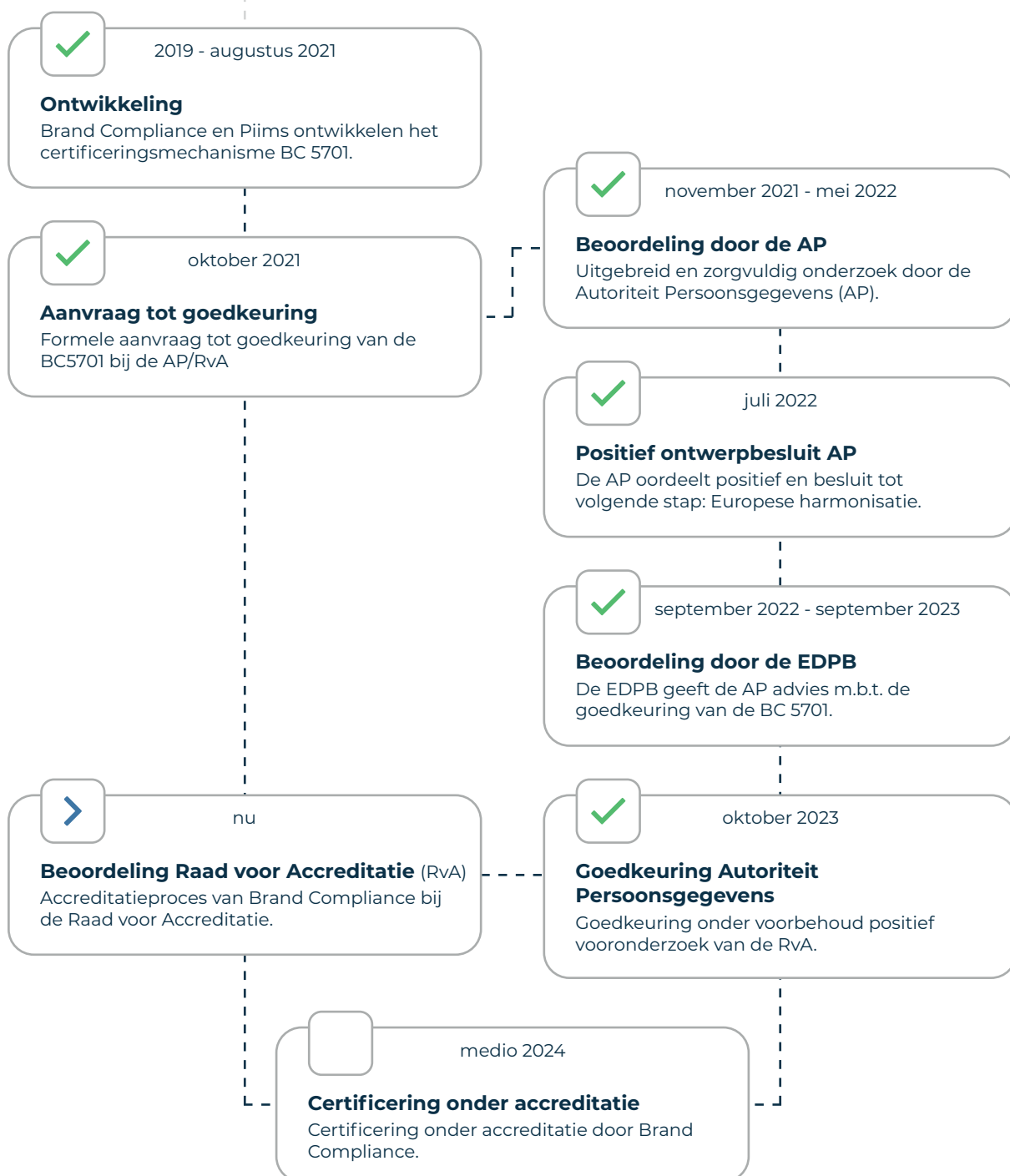
Bijlagen

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 en AP

Het goedkeuringsproces van de BC 5701

In oktober 2023, na een uitgebreid nationaal en Europees beoordelingsproces, heeft de Autoriteit Persoonsgegevens de AVG-Certificeringsstandaard BC 5701:2023 goedgekeurd. Dit betekent dat de Autoriteit Persoonsgegevens van mening is dat toepassing van deze criteria leidt tot een aantoonbaar passende uitwerking van de AVG. Onderstaand schetsen van het verloop van het goedkeuringsproces. Toekomstige termijnen zijn inschatting o.b.v. onze ervaring tot nu toe.



De BC 5701, (niet) voor iedere organisatie

Iedere organisatie die persoonsgegevens verwerkt kan vanaf nu met de 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. Ons advies: benader de bescherming van persoonsgegevens als een kwaliteitsaspect van de reguliere operatie en niet als een 'feestje van de staf'. Het borgen van de AVG-compliance vanuit de reguliere werkprocessen zorgt ervoor dat het altijd een punt van aandacht is en niet alleen wanneer de staf de organisatie daarop wijst. Het zorgt er ook voor dat zelfs de certificerings-audit geen verrassingen boven water halen en 'slechts' de aanleiding worden voor een feest!

Nu is het moment om de slag te slaan

Zoals gezegd kunnen we niet precies aangeven hoe lang accreditatie van Brand Compliance precies gaat duren. Maar laat u dat 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. Dus wil u straks een van de eerste organisaties in Nederland (en Europa) zijn die AVG-gecertificeerd zijn? Dan moet u nu starten met het implementatietraject.

Leidraad voor certificering

De AVG Certificeringsstandaard en -criteria BC 5701:2023 is de leidraad met eisen waaraan organisaties moet voldoen om voor het certificaat in aanmerking te komen.

De standaard beslaat ruim 180 pagina's (NL-versie) en is voor € 245,- excl. btw als PDF in het Nederlands en 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 aan de AVG 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 Implementatie Professional;
- 2 uit laten voeren door Brand Compliance.

De ervaring tot nu toe heeft ons geleerd dat de impact van de BC 5701 makkelijk wordt onderschat. Wij adviseren daarom ook om te kiezen voor optie twee of drie. U wilt er namelijk niet pas tijdens de certificatieaudit achter komen wat de implementatiecriteria van de BC 5701 echt betekent 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 vanaf nu opleidingen aan voor verschillende rollen met betrekking tot de implementatie. Hierin leren de deelnemers de 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 de technische uitvoering van de verwerking en bescherming van persoonsgegevens en een aantal technische aspecten m.b.t. aantoonbaarheid. 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 ‘tussentijdse beoordelingen’. Ook de tussentijdse beoordelingen worden uitgevoerd door een multidisciplinair auditteam. Tijdens de tussentijdse beoordelingen 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 certificatieaudit en twee tussentijdse beoordelingen. Aan het einde van de driejaarstermijn kan de organisatie kiezen voor hercertificering, waarmee de cyclus opnieuw begint.



Het BC 5701 certificaat maakt de kwaliteit en integriteit van uw gegevensverwerking zichtbaar voor alle belanghebbenden.

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 is 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 is kernauteur van de 'AVG Certificeringsstandaard en -criteria BC 5701:2023' en zet deze kennis in om mensen en organisaties te helpen bij het aantoonbaar passend uitwerken van de AVG. Piims Academy ontwikkelt en verzorgt alle officiële opleidingen m.b.t. de BC 5701.

Meer informatie vindt u op: www.piims.nl



Heb jij de ambitie om jouw organisatie met de verwerking van persoonsgegevens op de kaart te zetten? Op de volgende pagina staan de opleidingen die je daarbij kunnen helpen.

De volgende sessies en opleidingen zijn beschikbaar:

BC 5701 voor besluitvormers	BC 5701 Counselor
⌚ Duur: ½ dag 📋 Verkennen van de belangrijkste kansen en uitdagingen van de standaard. 🎯 Doelgroep: besluitvormers	⌚ Duur: 3 dagen 📋 Leert je de adviesrol m.b.t. de BC 5701 juist en zuiver in te vullen 🎯 Doelgroep: juristen en FG's
Implementatie Professional (FT)	Implementatie Professional (PG)
⌚ Duur: 6 dagen (Fast Track) 📋 Certificeringswaardig implementeren voor ervaren implementatiemanagers 🎯 Doelgroep: implementatie consultants	⌚ Duur: 10 dagen (Toegepaste Leergang) 📋 Parallel leren en implementeren met feedback op je implementatie. 🎯 Doelgroep: product owners en projectmanagers
BC 5701 Intern Auditor	BC 5701 Benchmark
⌚ Duur: 4 dagen 📋 Voor Implementatie Professionals die willen auditeren of hun kennis verder willen verdiepen 🎯 Doelgroep: auditoren en consultants	⌚ Duur: 4 dagen 📋 Niet certificeren maar de standaard leren gebruiken als benchmark voor het passend uitwerken van de AVG 🎯 Doelgroep: privacy professionals

Meer informatie over de opleidingen en ondersteuning vindt je op: www.piims.nl



www.brandcompliance.com
info@brandcompliance.com



www.piims.nl
info@piims.nl