AVG Garant

Checklist voor de te inspecteren onderneming

In deze checklist zijn de documenten opgenomen die door de onderneming minimaal 14 dagen voor de datum van de audit digitaal moeten worden aangeleverd.

Doc.nr	Wat	Aangeleverd
1	Uittreksel, van de onderneming, uit het Handelsregister van de Kamer van Koophandel. Deze mag op de datum van de audit niet ouder dan 3 maanden zijn.	
2	Organogram van de onderneming, inclusief functies en verantwoordelijkheden	
3	Meest recente versie van het door de onderneming opgestelde en goedgekeurde privacybeleid (gedocumenteerd en schriftelijk)	
4	Beschrijving van de wijze van interne communicatie van het privacybeleid binnen de onderneming	
5	Het door de onderneming opgestelde verwerkingenregister * In geval van verwerkingen buiten de EER tevens het beleid.	
6	Een overzicht van de door de onderneming gebruikte applicaties en systemen waarin persoonsgegevens worden vastgelegd. *NB: Van na mei 2018 in gebruik genomen en/of gewijzigde applicaties en systemen moet worden aangetoond dat bij de ontwikkeling rekening is gehouden met privacy beginselen en risico's ("privacy by design of privacy by default)*	
7	Beschrijving van het informatiebeveiligingsbeleid, inclusief beschrijving van de toegepaste beveiligingsmaatregelen	
8	De door de onderneming binnen de verschillende applicaties en systemen gehanteerde autorisatieschema's (wie mag wat)	
9	Het door de onderneming opgestelde (en gepubliceerde) privacy statement	
10	Door de onderneming opgestelde procedures en werkinstructies met betrekking tot de verwerking van persoonsgegevens	
11	Overzicht van de afgesloten verwerkersovereenkomsten met alle partijen waarbij de onderneming als verwerkingsverantwoordelijke verwerkingen uitbesteed aan een verwerker *NB: De auditor zal tijdens de audit een aantal verwerkersovereenkomsten opvragen ter beoordeling. De verwerkersovereenkomsten dienen tijdens de audit beschikbaar te zijn.*	
12	Verslagen en resultaten van door de onderneming bij verwerkers uitgevoerde beoordelingen met betrekking tot de prestaties en compliance van deze verwerkers	
13	Beschrijving van de incidenten- en datalekprocedure en de wijze van vastlegging.	
14	Overzicht van de geregistreerde incidenten- en datalekken over de afgelopen 12 maanden, inclusief de aan de Autoriteit Persoonsgegevens gemelde datalekken.	
15	Overzicht van door de medewerkers van de onderneming gevolgde trainingen op het gebied van privacy	
16	Procedurebeschrijving met betrekking tot het uitvoeren van rechten van betrokkenen (inzage, rectificatie en wissing van gegevens)	
17	Overzicht van de geregistreerde verzoeken van betrokkenen over de afgelopen 12 maanden	
18	Indien van toepassing: Overzicht van uitgevoerde DPIA's (Data Protection Impact Assessment) voor hoog risicovolle verwerkingen.	
19	Het bewaarbeleid van de onderneming, inclusief een overzicht van de gehanteerde bewaartermijnen per soort document	
20	Beschrijving van de procedure ten aanzien van het juist houden van gegevens	
21	Verslagen en resultaten van de door onderneming uitgevoerde privacy audits	