Inhoudsopgave

Inleiding

Voor u ligt het Werkboek bij Grip op de AVG. In de eerste acht hoofdstukken van Grip op de AVG hebben we u aan de hand genomen bij een tocht door de Algemene Verordening Gegevensbescherming. Het negende hoofdstuk gaf concrete handvatten om in uw organisatie ook daadwerkelijk met de AVG aan de slag te gaan.

Dit werkboek is bedoeld als ondersteuning bij dat negende hoofdstuk. Want wie daadwerkelijk aan de slag gaat, merkt al snel dat er beleid, procedures en afspraken nodig zijn. En dat er een overzicht nodig is van de belangrijkste zaken waarop gestuurd moet worden. Het werkboek voorziet voor een deel in deze leemte met een aantal sjablonen en handreikingen die als basis voor de benodigde documentatie kunnen dienen. En ook met een *control framework*, een overzicht van typische *controls* waarop veel organisaties in hun privacymanagement op zullen willen sturen. U kunt deze als uitgangspunt nemen en uitwerken voor en toespitsen op uw eigen organisatie. In de sjablonen en handreikingen is behalve met de AVG ook rekening gehouden met de huidige privacywetgeving. Overigens presenteren we u het control framework in de vorm van een vragenlijst, die bij uitstek geschikt is voor het doen van een nulmeting op de staat van privacy in uw organisatie. Door de vragen om te zetten naar beweringen ontstaat een daadwerkelijke lijst van controls.

Sjablonen en handreikingen zijn natuurlijk nog geen uitgewerkte documenten. Ter inspiratie hebben we één zo'n volledige uitwerking toegevoegd, te weten het sjabloon Procedure incidentenbeheer.

Op de volgende bladzijde leest u hoe u de beschikking kunt krijgen over bewerkbare elektronische versies van de documenten in dit werkboek.

Neem contact met ons op via www.privacymanager.nu/contact als u ook geautomatiseerd met het control framework aan de slag wilt gaan!

1 Privacy control framework

Vragenlijst

Het overzicht van vragen met toelichting in dit document geeft een weergave van alle relevante aandachtspunten voor privacymanagement in de organisatie.

1.1 Governance

1.1.1 ACTIEF STUREN OP PRIVACY DOOR DE DIRECTIE

I	Heeft de directie een overkoepelend privacybeleid vastgesteld waarin zij haar visie op privacybescherming verwoordt en beschrijft hoe zij concreet waarborgt dat de organisatie gegevens rechtmatig, behoorlijk en transparant verwerkt?	Door het vaststellen van het privacybeleid door het topmanagement worden het privacybeleid en de verantwoordelijkheden op strategisch en uitvoeringsniveau geborgd.
II	Heeft de directie het vastgestelde privacybeleid, zoals hierboven beschreven, gecommuniceerd binnen de organisatie?	Het geformuleerde privacybeleid is alleen effectief wanneer de medewerkers op de hoogte zijn.
III	Is de directie voldoende op de hoogte van het privacybeleid dat geldt binnen de organisatie en de naleving van de privacyregelgeving, zowel op papier als in de praktijk, om hier op ieder moment verantwoording over af te kunnen leggen?	Het privacybeleid kan alleen effectief zijn wanneer de directie zich daar actief mee bezig houdt, en dus niet alleen op papier verantwoordelijk is.
IV	Evalueert de directie periodiek de doelmatigheid en de doeltreffendheid van het privacybeleid en de naleving van de privacyregelgeving?	Veranderende bedrijfsprocessen en omstandigheden vereisen veranderende privacywaarborgen. De manier om te controleren of het privacybeleid passend is, is het inzetten van een evaluatiesysteem.

V	Stuurt de directie het privacybeleid en de naleving van de privacyregelgeving aantoonbaar bij waar dat op grond van de evaluatie nodig is?	Veranderende bedrijfsprocessen en omstandigheden vereisen veranderende privacywaarborgen. De manier om te zorgen dat het privacybeleid passend blijft, is het inzetten van een herzieningssysteem.

1.1.2 GOVERNANCESTRUCTUUR

I	Is er een portefeuillehouder privacy binnen de directie?	De portefeuillehouder privacy is eindverantwoordelijk voor een adequaat privacybeschermingsniveau en effectief privacymanagement binnen de organisatie.
II	Is voor alle afzonderlijke privacy waarborgende taken en processen duidelijk welke rol of functie daarvoor in de organisatie verantwoordelijk is?	Naast de portefeuillehouder privacy krijgen anderen binnen de organisatie de verantwoordelijkheid om privacy waarborgende taken en processen uit te voeren. Zoals het behandelen van verzoeken van betrokkenen, het coördineren van het privacyteam of het afhandelen van datalekken.
III	Zorgt de directie zorg voor slagvaardige collectieve regievoering in het geval van gemeenschappelijke verwerkers?	Het kan voorkomen dat meerdere verantwoordelijken een verwerker moeten aansturen. Bijvoorbeeld bij samenwerkingsverbanden. Heldere afspraken over de rolverdeling zijn dan noodzakelijk.
IV	Zorgt de directie voor voldoende toezicht op de uitvoering van het privacybeleid door de directie zelf, door de medewerkers en door derden?	De directie heeft niet de capaciteit, en heeft ook niet als taak, om toezicht te houden op de individuele verwerkingen. Wel dient zij ervoor te zorgen dat er voldoende toezicht georganiseerd is, en dat zij over de resultaten daarvan geïnformeerd wordt.

V	Biedt het privacybeleid voldoende concreet houvast voor het meten, controleren en optimaliseren van de privacybescherming?	De evaluatieprocedures uit de normen 1.1.1-IV en 1.1.1-V dienen te worden vastgelegd in het privacybeleid. Dit behelst niet alleen dat er geëvalueerd moet worden, maar onder andere ook de wijze en frequentie van evalueren, en het daarop volgende verbeterproces.
VI	Bevat het privacybeleid afspraken over de inbreng die de portefeuillehouder privacy heeft binnen de directie, zowel als onderdeel van de managementcyclus als ad hoc?	Er is een verschil tussen de portefeuillehouder privacy binnen de directie (bestuurlijke rol) en de privacycoördinator (uitvoerende rol). Om privacy als aandachtspunt in de organisatie te behouden dient het beleid aan te geven op welke vlakken de portefeuillehouder privacy inbreng heeft binnen de directie.
VII	Waarborgt het privacybeleid dat betrokkenen hun rechten, zoals op inzage en verbetering, eenvoudig uit kunnen oefenen?	Is het beleid begrijpelijk voor de betrokkenen en biedt het beleid ruimte voor betrokkenen om gebruik te mogen maken van hun rechten? Bijvoorbeeld in de vorm van selfservice via een beveiligd internetportaal.
VIII	Beschrijft het privacybeleid hoe de directie communiceert over het beleid zelf en de uitvoering ervan?	Het opstellen van interne en externe communicatieprocedures is essentieel voor een goede uitvoer van het privacybeleid. Daarnaast eist de AVG dat de organisatie op een zo goed mogelijke manier de relevante privacyaspecten naar de betrokkenen communiceert (dit kunnen dus zowel de medewerkers zijn als bijvoorbeeld klanten).
IX	Biedt het privacybeleid voldoende ruimte voor onafhankelijke rapportages over het beleid zelf en de uitvoering ervan door de toezichtverantwoordelijke?	Degene(n) belast met het toezicht op privacy binnen de organisatie moeten voldoende ruimte hebben om hun taak goed uit te voeren. Hieronder valt de mogelijkheid om rapporten op een onafhankelijke wijze op te stellen.

1.1.3 MIDDELEN

I	Voorziet de directie in de benodigde middelen voor het inrichten en uitvoeren van privacymanagement in de organisatie?	Degene(n) belast met de coördinatie en ondersteuning van privacyactiviteiten moeten voldoende mogelijkheden hebben om hun taak goed uit te voeren.
II	Voorziet de directie in de benodigde middelen voor proceseigenaren om hun processen privacybestendig te maken en houden?	Privacybescherming moet geen sluitpost zijn bij het vormgeven van processen.
III	Voorziet de directie in de benodigde middelen voor interne bewustwording en doelgroepgerichte training van medewerkers op privacybestendig werken?	Het creëren van bewustzijn, draagvlak en kennis van privacy onder de uitvoerders van de werkprocessen bevordert de effectiviteit van het privacybeleid.
IV	Voorziet de directie in de benodigde middelen voor het faciliteren van privacyservices?	Bij deze vraag is van belang of de directie voldoende en aantoonbaar voorziet in de middelen voor de facilitering van de rechten van de betrokkenen, zoals het recht op inzage.
V	Voorziet de directie in de benodigde middelen voor publieksvoorlichting?	De AVG vereist dat de organisatie op een zo goed mogelijke manier de relevante privacyaspecten naar de betrokkenen communiceert. Dit kunnen zowel werknemers zijn als bijvoorbeeld klanten.
VI	Voorziet de directie in de benodigde middelen voor adequaat en onafhankelijk toezicht?	Degene(n) belast met het toezicht op privacy binnen de organisatie moeten voldoende ruimte hebben om hun taak goed uit te voeren. Hieronder valt de mogelijkheid om rapporten op een onafhankelijke wijze op te stellen.

1.2 Organisatie van privacy

1.2.1 PRIVACYCOÖRDINATIE

I	Heeft de organisatie een privacycoördinator (privacymanager, privacy officer) aangesteld?	De privacycoördinator overziet, coördineert en ondersteunt privacy gerelateerde processen in de organisatie.
II	Is er een functieprofiel van de privacycoördinator beschikbaar?	
III	Heeft de privacycoördinator de mogelijkheid om gevraagd of ongevraagd de directie te informeren over de stand van zaken op het gebied van privacy?	De mogelijkheid tot initiatief van de privacycoördinator draagt bij aan het tijdig ontdekken en verbeteren van inefficiënt of inadequaat privacymanagement.
IV	Heeft de privacycoördinator voldoende tijd en middelen voor zijn eigen opleiding, training en begeleiding?	De veranderingen in het privacydomein maken het regelmatig bijspijkeren van privacykennis noodzakelijk.
V	Is er een team (incl. overlegorgaan) met toereikende kennis en ervaring op privacygebied dat het management adviseert?	In veel gevallen zal dit een Privacy Informatiebeveiligingsteam (PIT) zijn, wat kan bestaan uit vertegenwoordigers van onder meer de afdelingen juridische zaken, informatiebeveiliging, risicomanagement, audit, compliance, ICT en Inkoop.

1.2.2 FUNCTIONARIS GEGEVENSBESCHERMING

In artikel 38 AVG zijn enkele vereisten opgenomen die horen bij het aanstellen van een FG. Die zijn in deze norm uitgewerkt. De controls in dit onderdeel zijn alleen van toepassing voor organisaties die verplicht zijn om een FG aan te stellen, of die ervoor kiezen om dat vrijwillig te doen. Het aanstellen van een FG is verplicht voor overheidsorganisaties en voor organisaties die op grote schaal bijzondere persoonsgegevens verwerken of aan stelselmatige observatie doen.

I	Is een Functionaris voor Gegevensbescherming aangesteld?	
II	Maakt de organisatie bij het aanstellen van de FG zijn of haar contactgegevens bekend aan de AP?	

III Heeft de FG de mogelijkheid om rechtstreeks aan de hoogst leidinggevende binnen de organisatie verslag uit te brengen?

IV Betrekt de organisatie de FG tijdig en naar behoren bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens?

V Ondersteunt de organisatie de FG bij de vervulling van zijn of haar taken door de FG toegang te verschaffen tot de persoonsgegevens, verwerkingsactiviteiten en door de benodigde middelen ter beschikking te stellen?

VI Garandeert de organisatie de onafhankelijkheid van de FG door geen instructies aan de FG af te geven met betrekking tot de uitvoering van zijn of haar taken en door hem/haar ontslagbescherming te geven en hem/haar te vrijwaren van
mogelijke repercussies naar aanleiding van de uitvoering van zijn of haar taken?

VII Wordt de FG gehouden aan een geheimhoudingsplicht met betrekking tot het uitvoeren van zijn of haar taken?

VIII Garandeert de organisatie dat geen van de taken en plichten van de FG tot een belangenverstrengeling voor de FG zullen leiden?

1.2.3 RISICOMANAGEMENT

I Heeft de organisatie een risicoanalyse uitgevoerd op de werkprocessen om de impact op de organisatie en de betrokkenen te achterhalen?

Het gaat hier om een organisatie-PIA. Het bestuur en management dienen een goed beeld te hebben welke hoofdprocessen (thema's) bijzondere aandacht nodig hebben in het kader van privacybescherming en welke prioritering daar aan gegeven moet worden.

II	Heeft de organisatie een implementatieplan privacy vastgesteld (gebaseerd op een nulmeting en gap- en impactanalyse) waarin voor het komende jaar is aangegeven welke acties noodzakelijk zijn op het gebied van privacy?	Een nulmeting legt de organisationele gebieden bloot waar privacy onvoldoende is geregeld. Naar aanleiding van deze meting wordt een plan opgesteld om de nodige verbeteringen aan te brengen.
III	Is duidelijk op welke werkprocessen aanvullend PIA's uitgevoerd moeten worden en is daarvoor een planning opgesteld?	Niet alleen de overkoepelende stand van zaken wat betreft privacy dient gemeten en op niveau gebracht te worden. Het is noodzakelijk dit ook op procesniveau te doen.
IV	Beschikt de organisatie over de mogelijkheid om intern (onafhankelijk) onderzoek te doen naar de naleving van getroffen maatregelen op het gebied van privacybescherming?	Degene(n) belast met het toezicht op privacy binnen de organisatie moeten voldoende ruimte hebben om hun taak goed uit te voeren. Hieronder valt de mogelijkheid om onderzoek op een onafhankelijke wijze te doen.
V	Bestaat er een risicomanagementrapportage die duidelijk vermeldt in welke mate de organisatie de privacyrisico's in lijn heeft gebracht of brengt met het privacybeleid?	Het is raadzaam om de risico's rond werkprocessen helder in kaart te hebben en te beschrijven hoe de omgang met deze risico's in het privacybeleid past.

1.2.4 VERWERKINGSREGISTER

I	Beschikt de organisatie over een register van alle verwerkingsactiviteiten?	Art. 30 AVG stelt een dergelijk register verplicht.
II	Bevat het verwerkingsregister alle verplichte informatie?	Zie art. 30 lid 1 AVG.
III	Beschikt de organisatie over een procedure voor het actueel houden van het verwerkingsregister?	

1.2.5 PRIVACY IMPACT ASSESSMENTS (PIA'S)

I	Zijn voor specifieke processen binnen de organisatie PIA's uitgevoerd?	Voor processen waarbij op grote schaal bijzondere persoonsgegevens worden verwerkt, waarbij sprake is van stelselmatige observatie of waarbij gebruik wordt gemaakt van geautomatiseerde besluitvorming gebaseerd op persoonlijke aspecten, is het uitvoeren van een PIA voor een verantwoordelijke verplicht.
II	Worden PIA's op werkprocessen/thema's aantoonbaar uitgevoerd volgens een geldende standaardaanpak met bijbehorende checklists?	De standaardaanpak garandeert dat de PIA effectief is en niet een onjuist gevoel van veiligheid biedt op het gebied van privacy.
III	Is er een procesbeschrijving voor het uitvoeren van PIA's en het opvolgen van de uitkomsten?	Het is raadzaam om een PIA in een zo vroeg mogelijk stadium uit te voeren. Hoewel de PIA gedefinieerd is als een analyse die plaatsvindt per specifieke verwerking van persoonsgegevens, kan ook een ander abstractieniveau gekozen worden, bijvoorbeeld door te kijken naar een of meerdere bedrijfsprocessen.
IV	Is van elke uitgevoerde PIA een rapportage beschikbaar en heeft de proceseigenaar deze voor akkoord ondertekend?	De resultaten van de PIA moeten verifieerbaar en vindbaar zijn.
V	Is op basis van de PIA-rapportage een plan van aanpak opgesteld voor passende (technische en/of organisatorische) maatregelen?	Een PIA legt de onderdelen van processen bloot waar privacy onvoldoende is geregeld. Naar aanleiding van deze meting wordt een plan opgesteld om de nodige verbeteringen aan te brengen.
VI	Wordt aantoonbaar opvolging gegeven aan de aanbevelingen/verbetervoorstellen uit de PIA's?	Risicoanalyses worden periodiek uitgevoerd. Door het afstemmen van de risicomanagementcyclus met de begrotingscyclus is eenvoudig opvolging van de bevindingen van de risicoanalyse in de begroting mogelijk. Doordat de PIA meestal alleen wordt uitgevoerd bij nieuwe verwerkingen of bij veranderin-

gen in de verwerking van de persoonsgegevens, is opvolging in de begrotingscyclus hierbij vanzelfsprekend.

1.2.6 COMPLIANCEPROCES

I	Is er rond de beheersing van de privacybescherming een proces gebaseerd op plan-do-check-act-cyclus dat op basis van rapportages de directie voorziet in tijdige stuur- en verantwoordingsinformatie?	Door het plannen en organiseren van evaluatiecycli is de organisatie in staat om het privacybeleid actueel te houden.
II	Zijn er waarborgen dat het privacybeleid en de uitvoering ervan tijdig worden herijkt?	Zekerheid over het plaatsvinden van de evaluaties, evenals de regelmaat ervan, is nodig om het privacybeleid en de uitvoering ervan actueel te houden
III	Wordt bij het ontwerp en de inkoop van gegevensverwerkende processen en systemen rekening gehouden met het vermijden van privacyrisico's door het toepassen van Privacy by Design en Privacy by Default?	Bij het ontwerp en de inkoop van gegevensverwerkende processen en systemen wordt bijvoorbeeld in vroege fasen gescreend op een "passend" of "adequaat" beveiligingsniveau conform het eigen privacybeleid. Privacyrisico's kunnen na een belangenafweging worden geadresseerd en dusdanig vermijd of 'gecontroleerd' worden tijdens het ontwerp of de aanname van het gegevensverwerkende proces of systeem.
IV	Is er een procedure voor het contracteren van verwerkers?	Aan het verwerken van persoonsgegevens door een derde (in de AVG een 'verwerker'), zijn wettelijke voorwaarden verbonden. De verantwoordelijke organisatie is bijvoorbeeld verplicht compliant te zijn met de AVG, en door schriftelijke afspraken op te nemen over onder andere de te nemen beveiligingsmaatregelen voldoet de verantwoordelijke hieraan. De organisatie zou een procedure moeten opstellen inzake welke stappen er doorlopen moeten worden voordat een verwerker gecontracteerd wordt.

V	Is er een procedure of protocol voor het waarborgen van de kwaliteit van de set persoonsgegevens die wordt vastgelegd?	De verantwoordelijke draagt zorg voor de accuraatheid van de persoonsgegevens die zij beheert. De betrokkene kan hierbij om inbreng worden gevraagd.
VI	Is er een procedure of protocol voor het vaststellen van bewaartermijnen, en voor het vernietigen van persoonsgegevens nadat de bewaartermijn is overschreden?	Persoonsgegevens mogen, met enkele uitzonderingen, niet langer dan noodzakelijk bewaard worden. Hier dient rekening mee te worden gehouden bij het vaststellen van bewaartermijnen.
VII	Lopen er programma's voor communicatie en bewustzijn rondom privacy?	De verantwoordelijke is verplicht te communiceren met alle stakeholders over het privacybeleid en de gevolgen ervan.
VIII	Is duidelijk wie het aanspreekpunt is voor de externe toezichthouder (AP)?	Deze persoon (idealiter de Functionaris Gegevensbescherming) overlegt zo nodig met de AP over bijzondere verwerkingen en kan het beleid verantwoorden naar de toezichthouder.
IX	Zijn de gedragsregels voor het personeel van de organisatie afgestemd op de eisen vanuit de AVG (do's en don'ts)?	De integriteitscoördinator is doorgaans belast met de gedragsregels die van toepassing zijn op alle werknemers (intern en extern) die werkzaam zijn bij de organisatie.

1.2.7 SAMENWERKINGSVERBANDEN

I	Doet de organisatie aantoonbaar navraag naar de privacybeleidsuitvoering ingeval de organisatie een samenwerking aangaat met andere organisaties?	Om de integriteit met betrekking tot privacy in stand te houden voert de organisatie voor elke samenwerking een check uit bij de andere partij.
II	Ziet de organisatie af van samenwerking wanneer blijkt dat een aanbieder onvoldoende privacybestendig is?	De navraag alleen is niet voldoende, zijn er ook gevolgen aan verbonden wanneer blijkt dat de andere partij inadequaat met privacy omgaat?