omgevingsdienst nhn

JAARRAPPORTAGE GEGEVENSBESCHERMING

Betreft tijdvak 15 juni 2020- 15 maart 2021.
Status: definitief

OPSTELLER

Organisatie	: Omgevingsdienst Noord-Holland Noord
Afdeling	: Concernondersteuning
Functionaris gegevensbescherming	: Jan Kramer
Telefoon	: 06 5353 4332
E-mail	: jkramer@odnhn.nl
Kenmerk	: Jaarverslag AVG
Adres	: Postbus 2095
	1620 EB HOORN
Bezoekadres	: Dampten 2
	: 1624 NR HOORN

OPDRACHTGEVER

Organisatie	: Dagelijks bestuur OD NHN
Portefeuillehouder	: Klik en typ Contactpersoon
Telefoon	: Klik en typ Telefoonnummer opdrachtgever
E-mail	: Klik en typ E-mailadres opdrachtgever

DATUM

15 maart 2021

INHOUDSOPGAVE

1 VOORWOORD

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. In de AVG en de uAVG is het wettelijk kader beschreven voor het verwerken van persoonsgegevens. Persoonsgegevens mogen alleen worden verwerkt wanneer dit in overeenstemming is met het doel waarvoor zij zijn verzameld. Gegevens mogen niet langer bewaard worden dan strikt noodzakelijk. De organisatie dient transparant te zijn welke persoonsgegevens zij verwerkt en voor welk doel.

De Omgevingsdienst NHN (OD NHN) dient als overheidsinstantie zorgvuldig om te gaan met persoonsgegevens. De OD NHN verwerkt bij de uitoefening van haar taken veel informatie voor de deelnemende gemeenten en de provincie. Niet alleen persoonlijke informatie van de inwoners, maar ook van andere burgers, medewerkers, externen ketenpartners en zakenrelaties. De organisatie moet passende, technische en organisatorische beveiligingsmaatregelen treffen om onrechtmatige toegang tot deze persoonsgegevens tegen te gaan en daardoor onrechtmatig gebruik van deze persoonsgegevens te voorkomen. Daarnaast heeft de organisatie bij de uitvoering van haar taken ook te maken met tal van privacyregels in de sectorspecifieke wetgeving. Dit alles heeft gevolgen voor de inrichting van de processen en systemen van de OD NHN.

Naast de externe toezichthouder (de AP) dient de OD NHN als overheidsinstantie te beschikken over een interne toezichthouder: de Functionaris voor de Gegevensbescherming (FG). Op 15 juni 2020 heeft er een wisseling van de Functionaris Gegevens bescherming plaatsgevonden en is de heer Jan Kramer van de organisatie JAMsolutions (op interimbasis) als Functionaris Gegevensbescherming aangesteld.

De FG ziet erop toe dat de AVG intern wordt nageleefd. Het dagelijks bestuur dient erop toe te zien dat de FG naar behoren en tijdig wordt betrokken bij alle gelegenheden die verband houden met de bescherming van persoonsgegevens. Daarnaast dient de FG ondersteund te worden door hem toegang te verschaffen tot persoonsgegevens en verwerkingen daarvan en hem de benodigde middelen ter beschikking te stellen voor het vervullen van de taak en het in standhouden van zijn deskundigheid. Het dagelijks bestuur heeft dit in opdracht gegeven aan de directeur van de OD NHN.

De FG brengt jaarlijks een verslag uit aan de verwerkingsverantwoordelijke van zijn werkzaamheden en bevindingen en doet hij naar aanleiding daarvan aanbevelingen. Dit jaarverslag is bedoeld voor het Dagelijks Bestuur. Met dit jaarverslag kan het Dagelijks Bestuur haar verantwoording over dit onderwerp afleggen aan het Algemeen Bestuur.

In de AVG wordt het wettelijk kader beschreven voor het verwerken van persoonsgegevens. Zo dient de organisatie transparant te zijn welke persoonsgegevens zij verwerkt en voor welk doel. Persoonsgegevens mogen alleen worden verwerkt wanneer dit in overeenstemming is met het doel waarvoor zij zijn verzameld en gegevens mogen niet langer bewaard worden dan strikt noodzakelijk. Bovendien moet de organisatie passende technische en organisatorische beveiligingsmaatregelen treffen om onrechtmatige toegang tot deze persoonsgegevens tegen te gaan en daardoor een onrechtmatig gebruik van deze persoonsgegevens te voorkomen. Daarnaast heeft de OD NHN ook te maken met tal van privacyregels in sectorspecifieke wetgeving (denk aan de BOA’s bij handhaving). Dit alles heeft gevolgen voor de inrichting van processen en systemen.

2 LEESWIJZER

Deze rapportage bestaat uit twee onderdelen.

• Het eerste deel is een terugblik naar de periode 15 juni 2020 tot 1 januari 2021. Wat heeft de ODNHN bereikt op het gebied van gegevensbescherming? Welke maatregelen zijn er genomen om te voldoen aan de AVG?

• In het tweede deel worden aanbevelingen gedaan. Aanbevelingen om gegevensbescherming en privacy in het jaar 2021 naar een nóg hoger niveau te tillen. Hierbij wordt (waar nodig) tevens aandacht geschonken aan de technische en organisatorische maatregelen die nodig zijn om dit hogere niveau te bereiken. Voor 2021 staan er ook er ook een aantal grote wijzigingen op stapel waar vanuit AVG-oogpunt aandacht voor nodig is.

3 DEEL 1. TERUGBLIK OP 2020

De periode 15 juni 2020-31 december 2020 heeft een aantal veranderingen gekend op het AVG-gebied; de wisseling van de Functionaris Gegevensbescherming en het, sinds het uitbreken van de pandemie Covid-19, het van de een op de andere dag meer op afstand moeten gaan werken. Dit tijdvak heeft in het teken gestaan van brede bewustwording van de organisatie met privacy en de verschillende AVG-aspecten.

Privacy en gegevensbescherming zijn een bewust onderwerp geworden bij veel personen in de organisatie. Dat heeft voor de organisatie zeker bij het ineens meer op afstand moeten gaan werken haar vruchten afgeworpen. Individuele medewerkers hebben een alerte houding over de uitvoering van vraagstukken waarbij de privacy mogelijk in het geding komt. Uit eigen beweging zijn vraagstukken met betrekking tot de AVG en informatiebeveiliging door medewerkers aan de CISO en de FG voorgelegd. Daarmee zijn reparatiewerkzaamheden achteraf en potentiële datalekken voorkomen.

3.1 Het privacybeleid

Het hebben van een vastgesteld bestuurlijk privacy beleid is een wettelijke plicht waaraan sinds de ingang van de AVG 25 mei 2018 voldaan dient te worden. Het Bestuurlijk privacy beleid is afgestemd in de eigen organisatie en voorgelegd aan het Dagelijks Bestuur (DB). Hierop is een voorgesteld besluit van het DB aan het Algemeen Bestuur (AB) gedaan op 18-09-2019. Het AB heeft op 16-10-2019 conform voorstel het besluit overgenomen. Het bestuurlijk privacy beleid beschrijft hoe de OD NHN omgaat met persoonsgegevens en welke maatregelen zij treft om te voldoen aan de relevante wet- en regelgeving. Door de bekrachtig van het Bestuurlijk privacy beleid is hiermee het kader gegeven waarin de OD NHN aangeeft aan welke principes zij zich houdt bij de verwerking van persoonsgegevens.

3.2 Processen

De verwerking van persoonsgegevens dient te voldoen aan de wet, de AVG. Dit houdt in dat de werkprocessen die persoonsgegevens bevatten getoetst en ingericht moeten worden volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Daarnaast kan de OD NHN in bepaalde gevallen verplicht zijn om een Data Protection Impact Assessment (DPIA) uit te voeren.

Het maken en bijhouden van de procesbeschrijvingen is voor de OD NHN nog een leerproces wat moet groeien. Er zijn gedeeltelijk procesbeschrijvingen aanwezig. Deze zijn nog niet in overeenkomst met de beginselen van de wet en nog niet voor alle processen aanwezig. Dit houdt in dat de werkprocessen die persoonsgegevens bevatten getoetst en ingericht moeten worden volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Niet voor alle processen kan worden aangetoond dat ze voldoen aan de AVG-wet. Er dient hierbij overigens wel opgemerkt te worden dat dit niet wil zeggen dat er niet rechtmatig wordt gewerkt. Het maken/aanpassen van procesbeschrijvingen zal door de Directie van de OD NHN verder worden ingepland.

3.3 Organisatorische inbedding

Voor een goede en juiste uitvoering is het van belang dat eenieder binnen de organisatie op de hoogte is van de beginselen van de AVG en het belang van privacy. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustzijn creëren.

Kennis en kunde van de uitvoeringsaspecten van de AVG en (informatie)beveiliging is van essentieel belang. Dit voorkomt beveiligingsincidenten en datalekken, die veel tijd en aandacht vanuit het management vragen en die onnodige kosten met zich meebrengen. Van belang is dat iedereen op een basis- en soms op specialistisch kennisniveau wordt gebracht, zich bewust is van de risico's en zich vervolgens houdt aan de afspraken. Er is een campagne opgezet waarmee de bewustwording en kennis als continu proces in de organisatie wordt ingevoerd. Dit wordt ingezet met een verplicht en toch speels karakter. Medewerkers worden thematisch op praktische herkenbare wijze middels e-learning en i-Bewust zijn meegenomen naar een hogere bewustwording.

3.4 Privacy-management organisatie

De huidige bezetting van het "privacy team" is gebaseerd op externe inhuur. De organisatorische inbedding van de huidige externe functionarissen is goed er is een laagdrempeligheid gecreëerd waardoor de organisatie deze functionarissen voor tal van zaken weet te vinden. In de wetenschap dat de AVG-wetgeving en informatiebeveiliging niet meer weg is te denken en een steeds bredere aandacht krijgt bij het publiek, is een uitbreiding van "ambassadeurs" op de werkvloer in de vaste bezetting een invulling die de organisatie moet gaan overwegen. Dit draagt bij aan een verdere organisatorische borging en verankering van de privacywetgeving en het conform handelen.

3.5 Rechten van betrokkenen

De organisatie dient degene van wie zij de persoonsgegevens verwerkt (betrokkene) zowel actief als passief te informeren over het verwerken, de wijze van het verwerken, de grondslag en de maatregelen die zij neemt om onrechtmatige toegang en -verwerking te voorkomen. Daarnaast stelt de AVG dat betrokkenen in staat moeten zijn om middels een aantal rechten controle en invloed uit te kunnen oefenen over zijn of haar persoonsgegevens. De informatieplicht aan betrokkenen is nieuw terrein, en zit nog niet standaard in de communicatie en werkprocessen ingebed. De medewerkers doen het echter al wel. De completering hiervan zal worden meegenomen in de procesbeschrijvingen, werkinstructies en e-learning modules.

Er zijn in het genoemde tijdvak geen inzageverzoeken van betrokkenen binnen gekomen.

3.6 Intercollegiale samenwerking

Er is een intercollegiale samenwerking tussen de Functionarissen Gegevensbescherming en Privacy-officers van omgevingsdiensten in de regio. Tijdens bijeenkomsten komen diverse thema's, landelijke of regionale vraagstukken, het delen van kennis, voorbeelden en stukken aan de orde.

3.7 Samenwerking

De OD NHN werkt op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. In veelvoorkomende gevallen zal er sprake zijn van een verwerking van persoonsgegevens tussen partijen: ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens valt onder dit begrip. Deze verwerkingen dienen dan ook te voldoen aan de AVG. De OD NHN dient dan ook afspraken te maken met deze andere partijen.

3.8 Beveiliging

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat de OD NHN passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Daarnaast geldt er onder de AVG een meldplicht datalekken. Dit houdt in dat incidenten –waaronder inbreuken– op de beveiliging onder omstandigheden gemeld dienen te worden aan de AP en/of de betrokkene(n).

Het zorgdragen voor passende technische en organisatorische maatregelen is het afgelopen jaar sterk verbeterd. De ICT-omgeving is per 1 januari 2021 vervangen door een Microsoft Azure omgeving. Hierdoor is een belangrijke stap gezet naar de verdere modernisering van de ICT-infrastructuur en zijn volgens de maatstaven van de OD NHN voldoende uitgerust om te voldoen aan de wensen. Daarnaast is ook de Office 365 omgeving in gebruik genomen inclusief de Sharepoint omgeving voor dataopslag. Voor de overige zaken is een projectplan Informatiebeveiliging geschreven wat in het volgende tijdvak zijn uitvoering zal krijgen.

3.9 Datalekken

Er geldt binnen de AVG een meldplicht datalekken.

Bij de ODNHN dienen (vermoeden van) datalekken te worden gemeld via het intranet en/of telefonisch bij de Privacy Officer of de Functionaris Gegevensbescherming voor verder onderzoek. Niet ieder datalek behoeft gemeld te worden bij de AP, wel rust er een verplichting tot het bijhouden van datalekken. Dit houdt in dat incidenten –waaronder inbreuken– op de beveiliging onder omstandigheden niet gemeld hoeven te worden aan de AP en/of de betrokkene(n). Datalekmeldingen worden besproken tijdens het maandelijks overleg tussen de FG en de directie.

In de rapportage periode zijn er een aantal impactvolle datalekken geweest die volgens de criteria aan de AP gemeld zijn.

3.10 Verantwoording

De AVG legt de verantwoordelijkheid bij de organisatie zelf om aantoonbaar te maken dat deze voldoet aan de privacyregels. Door te voldoen aan de verantwoordingsplicht, levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy. Dit betekent dat het DB moet kunnen tonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en aan de relevante wet- en regelgeving.

Het opgestelde register van Verwerkingen, het datalekregister en het risicolog voldoen aan deze verantwoordingsplicht. De OD NHN is op dit onderdeel aantoonbaar compliant aan de AVG. Dit jaaroverzicht maakt onderdeel uit van haar verantwoordingsplicht.

3.11 Conclusie

Op hoofdlijnen kan de OD NHN aan haar verantwoordingsplicht voldoen. Er is weer veel en goed werk verzet. Op bepaalde onderdelen is er stagnatie en is er werk te doen zoals; organisatorische inbedding van de procesbeschrijvingen zodat die gaan voldoen aan de wetgeving (aantoonbaarheid), leveranciersmanagement en daaraan gerelateerde verplichting, Privacy-by design inrichting en informatiebeveiliging. Aan de kant van betere systemen en systeeminrichting, kennis en bewustwording, houding en gedrag zijn goede stappen gemaakt. Het compliant zijn aan de AVG-wetgeving is weer verder ingevuld, maar mag meer prioriteit krijgen op de onderdelen waarmee de aantoonbaarheid (lees: accountability) structureel en direct beschikbaar is vastgelegd.

4 DEEL 2. VOORUITKIJKEN NAAR 2021

De organisatie moet aantoonbaar voldoen aan de relevante wet- en regelgeving. Een organisatie zal continu aandacht moeten hebben voor de ontwikkeling van gegevensbescherming. In de huidige fase waarin de organisatie nog op veel terreinen in beweging is vraagt privacy en gegevensbescherming continu extra aandacht in dit proces. Het vraagt om structurele borging van dit onderwerp. Waar het tijdvak 2019-2020 in het teken stond van brede bewustwording zal 2020-2021 in het kader staan van toepassen, interpreteren en inbedden van de AVG. De periode 2020-2021 staat voor de organisatie in het teken van de implementatie en van veranderingen vanuit het masterplan ICT. Privacy en gegevensbescherming worden in de op handen zijnde veranderingen gewaarborgd. Alleen zo kan de organisatie uiteindelijk het huidig niveau behouden en aantoonbaar maken dat ze kan voldoen aan deze wet.

4.1 Het privacybeleid

Aanbevelingen:

Het privacy beleid is bestuurlijk vastgesteld door het DB en vervolgens het AB. Voor het managementteam ligt hier de taak om dit beleid actief uit te dragen en ervoor te zorgen dat medewerkers in staat worden gesteld dit beleid uit te kunnen voeren. Voorgenomen MT-besluiten moeten waar nodig getoetst worden aan de AVG eisen. Zorg voor voldoende formatieve bezetting en voor incidenteel-/structureel budget. Creëer een veilig klimaat waarin medewerkers beveiligingsincidenten durven te melden. In 2020 zal het privacy beleid geëvalueerd en eventueel geactualiseerd moeten worden.

4.2 Processen

Aanbevelingen:

Het advies is om alle bedrijfs- en werkprocessen inzichtelijk te maken, te starten met het in kaart brengen van de hoge risicoprocessen en dit prioriteit te geven. Deze overzichten tonen in een helder schema de route van een proces met de daarbij behorende gegevens en type uitwisselingen. Zorg hierbij dat dit voor iedereen toegankelijk is. Ook kunnen de wijzigingen die de invoering van de Omgevingswet verlangen dan gecontroleerd worden uitgevoerd. Van belang is dat in de processen aandacht wordt besteed aan wat gegevensbescherming en de privacywetgeving concreet betekenen voor de betreffende afdeling en hoe medewerkers om dienen te gaan met persoonsgegevens binnen de taken en werkzaamheden.

Het advies is om te controleren of medewerkers zich houden aan deze procesbeschrijvingen en of daarbij ondersteuning geboden kan worden als dit niet het geval is. Indien sprake is van mogelijk risicovolle (nieuwe) processen is het noodzakelijk dat de organisatie voorafgaand aan de gegevensverwerking een DPIA (lees: risicoanalyse) uitvoert. Het is de taak van de organisatie om inzichtelijk te maken wanneer een DPIA moet worden uitgevoerd en op welke wijze. De FG kan hierbij ondersteunen.

Privacy-by-design: Zorg ervoor dat, voordat er een verwerking van persoonsgegevens begint bij de inkoop of bij de start van een nieuw zaaktype, er een toets heeft plaats gevonden op grond van de AVG.

4.3 Organisatorische inbedding

Aanbevelingen:

De organisatorische inbedding kent afhankelijkheden met het Masterplan ICT. Zodra de organisatorische inbedding van de functies in het masterplan ICT een definitievere invulling kent, moet hier ook de definitieve bredere bezetting van een privacy team in de organisatie worden ingevuld. Binnen elke afdeling dient een privacy- en informatiebeveiligingsambassadeur aangewezen te zijn. Deze dient als aanspreekpunt voor de gehele afdeling en heeft nauw contact met het privacy team.

Het vaststellen van taken, verantwoordelijkheden en bevoegdheden binnen de organisatie als geheel is een aandachtspunt. Hiervan ligt weinig vast of is raadpleegbaar. Advies is hiervoor een sessie met het management te organiseren conform de ISO-standaarden. Dit moet verder geconcretiseerd worden.

4.4 Bewustwording

Aanbevelingen:

De AVG verplicht organisaties tijd en middelen ter beschikking te stellen voor kennis- en bewustwordingssessies. Advies is om trainingen te organiseren voor algemene kennis en voor specifieke doelgroepen (HR, leidinggevende en BOA's). Deze zullen nog worden ingepland. In ieder geval is van belang om toe te zien dat interne medewerkers de eed of belofte afleggen. Daarnaast dienen externe medewerkers een geheimhoudingsverklaring te hebben ondertekend.

4.5 Rechten van betrokkenen

Aanbevelingen:

Er zijn geen procesbeschrijvingen van de rechten van betrokkenen. De uitvoering van rechten van betrokkenen kan verbeteren als bij de start van het proces van gegevensdeling duidelijker wordt gecommuniceerd welke rechten de betrokkene heeft. Dit kan in de procesbeschrijving worden meegenomen en aan het begin van een formulier worden gepubliceerd. Daar waar gegevens worden verwerkt op basis van toestemming van de betrokkenen is dat onvoldoende bekend in de organisatie. Ook de daarbij behorende rechten zijn nog niet voldoende bekend. Deze kunnen in de opleiding en kennissessies verder worden opgepakt. Rechten medewerkers: ook werknemers hebben het recht te weten hoe en welke persoonsgegevens verwerkt worden. Voor deze doelgroepen kan een aparte privacyverklaring worden opgesteld.

4.6 Samenwerking

Aanbevelingen:

Bij het inschakelen van derden (ketenpartner, leverancier, collega organisatie etc.) is van belang te weten hoe deze zich verhouden tot de OD NHN. Dit in verband met de verschillende verantwoordelijkheden en aansprakelijkheden. De AVG kent rollen als 'Verantwoordelijke' en 'Verwerker' met eigen verplichtingen. Indien een nieuwe leverancier wordt ingeschakeld, of een nieuwe taak bij een bestaande leverancier, is van belang dat bekend is of, hoe en welke gegevens uitgewisseld worden. Deze moeten, voorafgaand aan de dienstverlening, in overeenkomsten waaruit de rechtmatigheid blijkt, worden vastgelegd. Hierbij heeft de (juridische) inkoopfunctie een belangrijke rol, maar tevens iedereen die contact heeft met ketenpartners. De lijst met verwerkersovereenkomsten is in 2020 geactualiseerd en zal jaarlijks worden gecontroleerd. Bij samenwerking met ketenpartners (bv RIEC of Veiligheidsregio's) is van belang dat daar een convenant voor is opgesteld waarin o.a. de rechtmatigheid van de verwerking getoetst is. Ook bij ad hoc bevragingen zorgt de OD NHN dan voor duidelijkheid over de rol van de derde partij. De organisatie maakt dienovereenkomstig afspraken met deze derde partij. De samenwerkingsovereenkomsten tussen de OD NHN en haar opdrachtgevers zijn nog niet formeel op het onderdeel gegevensuitwisseling specifiek gemaakt. Dit betreft vooral de afspraken indien een partij zich terugtrekt uit het de samenwerking. Advies is om deze overeenkomsten op te stellen.

4.7 Beveiliging

Aanbevelingen:

Beveiliging maakt onderdeel uit van de verplichtingen in de wet (art AVG 32). De organisatie is verplicht zodanige organisatorische en technische maatregelen te treffen dat de beschikbaarheid, vertrouwelijkheid en integriteit van gegevens en systemen adequaat beschermd zijn. De belangrijkste zaken die voor de OD NHN relevant zijn, zijn opgenomen in het Informatie beveiligingsplan (IB) wat weer is afgeleid van de BIO (baseline informatiebeveiliging overheid). In 2021 wordt verwacht dat de BIO geïmplementeerd is. De zaken die een relatie hebben met privacywetgeving zijn zeer urgent. Onderdelen hierin zijn, het invoeren van het in- en uitdienst proces, rol-gebaseerde toegang (niet meer kunnen zien dan voor je functie relevant is), en het incident- en changemanagementproces. Toets in ieder geval de beveiliging op meerder terreinen voor ingebruikname van de nieuwe omgeving.

4.8 Verantwoording

Aanbevelingen:

Voor elke verwerkingsactiviteit waarbij gegevens verwerkt worden op basis van toestemming, kan beter worden vastgelegd op welke manier de organisatie toestemming ontvangt, vastlegt en bewaart.

De organisatie kan transparanter zijn over de omgang met persoonsgegevens door bijvoorbeeld het verstrekken van informatiefolders bij aanvragen van producten en diensten. De OD NHN publiceert – bijvoorbeeld op de website – over de ontwikkelingen van de bescherming van privacy en de omgang met persoonsgegevens binnen de organisatie.

Door het uitvoeren van periodieke audits om de juiste werking van de getroffen beveiligingsmaatregelen te controleren kan beter worden voldaan aan de verantwoordingsverplichtingen.

Ook kan er rondom de AVG compliance een en ander worden opgenomen in het jaarverslag van de OD NHN.

4.9 Conclusies

Bij de OD NHN zijn de verplichtingen rondom de AVG voldoende geïmplementeerd en hierbij voldoet de OPD NHN aan haar wettelijke verplichtingen.

Van belang is, dat de organisatie continue deze verplichtingen blijft onderhouden. Onder andere door het up-to-date houden van de bewustwording van het personeel, zorgdragen voor het op orde hebben en houden van de primaire AVG huishouding (in de vorm het uitvoeren van DPIA's en het actueel houden van het verwerkingsregister en het datalekregister).