Hoogheemraadschap van Rijnland

Deze nota betreft het thema 'de opgaven van Rijnland'
Rijnland zorgt van oudsher voor droge voeten en schoon water. Door klimaatverandering stijgt de zeespiegel en extreme neerslag en droogte komen vaker voor. Rijnland neemt samen met inwoners en bedrijven doelmatige maatregelen om de gevolgen van klimaatverandering tegen te gaan.

Film de opgaven van Rijnland

Memo – Ter kennisname

Registratienummer:
18.076414

Aan:	VV
Van:	G.L. van Mourik
Onderwerp:	Stand van zaken AVG en restrisico's
Datum:	15-5-2018

Waarom moet u dit weten
Op 25 mei 2018 gaat de Algemene Verordening Gegevensbescherming (AVG) in werking.

Kernboodschap
Rijnland is hard aan het werk om compliant te worden met deze verordening.
De rechtmatigheid van de verwerking van persoonsgegevens door Rijnland is vastgesteld: voor de waterschappen is de grondslag voor verwerking van persoonsgegevens veelal de wettelijke taak, de uitvoering van een overeenkomst of een publieke taak.

De risico's zijn in beeld gebracht en de benodigde maatregelen om die te beheersen zijn vastgesteld. Wij geven u hierbij de stand van zaken van 15 mei.

Toelichting

Vanuit de VV is aandacht gevraagd voor de situatie bij de verbonden partijen, en met name bij BSGR, omdat die als verbonden partij met persoonsgegevens werkt.
BSGR is zelf verwerkingsverantwoordelijke en draagt zelf de verantwoordelijkheid om zorgvuldig met persoonsgegevens om te gaan. Rijnland en de BSGR hoeven daarom geen verwerkersovereenkomst af te sluiten.
Gelet op het feit dat het om gedelegeerde bevoegdheden gaat (bevoegdheden die Rijnland op afstand heeft gezet), is het enige dat Rijnland hierin kan doen: via onze bestuurder die in het AB/DB van BSGR zit erop toezien at de BSGR zich goed voorbereidt op de AVG. Wij hebben al kunnen constateren dat de BSGR zelf een FG heeft aangesteld en eveneens dat de BSGR Privacy-beleid heeft vastgesteld.
De overige verbonden partijen, het Waterschapshuis, Aquon en GR Slibverwerking verwerken geen van allen persoonsgegeven (voor Rijnland) . Richting deze partijen is vanuit Rijnland dan ook geen actie nodig in de zin van bijv. het afsluiten van een

verwerkersovereenkomst. Dat geldt eveneens voor partners waar wij andere (samen)werkrelaties mee hebben, zoals de Unie en de Waterschapsbank.

De **maatregelen** die Rijnland moet nemen zijn te verdelen in 8 onderdelen:

1. Communicatie

Medewerkers bewust maken van de benodigde zorgvuldigheid in het omgaan met persoonsgegevens: waarom worden die gegevens gebruikt en wat is uit oogpunt van zorgvuldigheid nodig om een datalek te voorkomen. Dit is een cruciale maatregel.

Via communicatie op Intranet worden medewerkers via 7 berichten vóór 25 mei vertrouwd gemaakt met de benodigde zorgvuldigheid. De eerste 6 berichten zijn al gepubliceerd.
Vóór 25 mei volgen alle medewerkers (en het dagelijks bestuur) een verplichte training op het gebied van het voorkomen en melden van datalekken (vóór de zomer volgt een 2e training).
Ook de betrokkenheid van medewerkers in het opstellen van werkinstructies (zie 2.) draagt bij aan de bewustwording.
We maken een digitale versie van het beleid, waarbij medewerkers gemakkelijk kunnen doorklikken naar meer/andere informatie.

2. Aanscherpen van procedures

Voor de werkprocessen moeten werkinstructies worden opgesteld. Dergelijke instructies helpen de medewerkers in het zorgvuldig handelen, waarmee de kans op datalekken afneemt.

Op basis van een algemene leidraad worden per proces werkinstructies opgesteld door de medewerkers die in dat proces actief zijn. Deze algemene leidraad is als bijlage opgenomen in het beleidsdocument. Per groep van processen is een coördinator/contactpersoon benoemd; zij zijn inmiddels geïnstrueerd, zodat de werkinstructies kunnen worden opgesteld.

3. Verwerkersovereenkomsten afsluiten

Persoonsgegevens waarvoor HHR en HHSK verantwoordelijk zijn kunnen ook aanwezig zijn bij derden of worden verwerkt door derden, zoals aannemers of beheerders van ICT-systemen.
Met dergelijke partijen wordt een verwerkersovereenkomst afgesloten; daarin wordt geregeld dat de betreffende partij zich houdt aan de AVG. Ook verwerkers die al een verwerkersovereenkomst hadden onder de WbP moeten een nieuwe verwerkersovereenkomst tekenen.
Dit geldt niet voor de verbonden partijen (met name de BSGR werkt natuurlijk veel met persoonsgegevens); zij zijn zelfstandig verantwoordelijk voor het voldoen aan de AVG.

Leveranciers hebben een eigen verantwoordelijkheid onder AVG. In de verwerkersovereenkomsten worden die verantwoordelijkheden afgestemd op de Rijnlandse verantwoordelijkheden.
De inventarisatie (welke leveranciers het betreft) voor grote leveringen, diensten en werken (groot is >= 50.000) is gereed, evenals de model-overeenkomst.

Voor kleinere overeenkomsten loopt de inventarisatie. De daadwerkelijke aanpassing van de bestaande contracten met leveranciers is gestart, maar deze actie zal waarschijnlijk niet klaar zijn op 25 mei.

4. Aanpassen organisatie
   a) een Functionaris gegevensbeheer (FG) moet worden aangesteld. Hij/zij ziet toe op de wijze waarop wordt voldaan aan de AGV;
   b) een incident response team (IRT) moet worden ingericht; dit team behandelt de gemelde datalekken.

Deze aanpassingen van de organisatie zijn doorgevoerd. Het IRT is bij Rijnland geen apart team maar maakt deel uit van het Kernteam Privacy.

5. Implementeren van ICT-maatregelen

De noodzakelijke ICT-maatregelen zijn voor zover nu bekend enerzijds aanpassingen in systemen (autorisaties goed instellen) en anderzijds de aanschaf en implementatie van een IAM-tool (een tool om systemen met persoonsgegevens van medewerkers te koppelen zodat vanuit één bron kan worden gewerkt voor die gegevens). Deze maatregelen ondersteunen de medewerkers in het voorkomen van datalekken.

Een IAM-tool wordt geïmplementeerd; daarmee wordt bereikt dat gegevens van medewerkers in één systeem zitten en worden beheerd.
De noodzakelijke aanpassingen in systemen worden nog geïnventariseerd. Vervolgens wordt in kwartaal 3 van 2018 een planning voor de realisatie van die aanpassingen opgesteld Deze ondersteunende maatregelen zijn dus niet afgerond op 25 mei.

6. Registers

In registers moeten diverse zaken worden vastgelegd, zoals waar persoonsgegevens zijn opgeslagen, welke autorisaties zijn verstrekt en welke verwerkersovereenkomsten er zijn.
Voor monitoring en evaluatie worden nog afspraken gemaakt.

Er is een model gekozen en diverse voorbeelden zijn ter toelichting erin opgenomen. Eind april is gestart met het vullen van het register door de vakafdelingen. Deze actie zal vóór 25 mei zijn afgerond.

7. Procedure datalekken

Er is een "procedure datalekken" nodig die beschrijft hoe moet worden gehandeld als er een datalek is (N.B. er is sprake van een datalek als persoonsgegevens verloren zijn gegaan of als onbevoegden toegang hebben tot persoonsgegevens).

De "procedure datalekken" is gereed. Via Intranet kunnen medewerkers inmiddels een datalek melden.
Het kernteam Privacy zorgt dan, zo nodig, voor melding bij de Autoriteit Persoonsgegevens, belegt het dichten van het datalek bij de betreffende proceseigenaar en houdt toezicht daarop. Deze aanpak is opgenomen in het Incident Response Protocol.

8. Beleid opstellen

In het beleid ter bescherming van persoonsgegevens is opgenomen hoe HHR en HHSK omgaan met persoonsgegevens. Daartoe is elders al vastgesteld beleid als basis gebruikt.

Het concept is in 2 rondes besproken met poho en DT en is op 15 mei in D&H vastgesteld.
Het Privacystatement voor internet is gepubliceerd op de internetsite van Rijnland.

De restrisico's
Persoonsgegevens bevinden zich in veel processen en bestanden. De kans is reëel dat op 25 mei niet 100 % in beeld is waar al die gegevens zitten. Met name de bewustwording bij medewerkers op het vlak van omgaan met persoonsgegevens is daarom cruciaal. Daar is al veel aandacht aan besteed en dat proces gaat door.
Naarmate ondersteunende maatregelen verder zijn doorgevoerd zal het risico wel structureel minder zijn.

De belangrijkste risico's na 25 mei zijn:

- Datalek: persoonsgegevens komen terecht bij iemand die daar niets mee te maken heeft. De beheermaatregel is de procedure voor datalekken. Er zijn regels vanuit de Autoriteit Persoonsgegevens (AP) voor de melding van dergelijke lekken. Gelet op de beperkte menscapaciteit zal de AP slechts in een beperkt aantal situaties kunnen toetsen hoe wordt omgegaan met een datalek.
- Verzoek van betrokkene: mensen van wie persoonsgegevens worden gebruikt door Rijnland kunnen vragen wat daarmee gebeurt, in welke systemen ze zitten en kunnen vragen om gegevens te verwijderen (geldt niet altijd voor alle gegevens). Als betrokkene van mening is dat het verzoek niet adequaat is behandeld dan kan hij/zij dat melden bij de AP. Hoe de AP daarmee omgaat staat al beschreven bij "datalek".
- Verwerkersovereenkomsten: niet alle verwerkersovereenkomsten zullen zijn aangepast; dat kan zijn omdat er discussie is over de standaardtekst van Rijnland of omdat nog niet alle overeenkomsten in beeld zijn. Gelet op de wettelijke eigen verantwoordelijkheid van leveranciers wordt het risico hier gering geacht.
- ICT-maatregelen: de ICT-maatregelen zijn erop gericht dat medewerkers alleen die gegevens kunnen inzien die relevant zijn voor hun functie. Die maatregelen vormen daarmee een ondersteuning van het bewust omgaan met persoonsgegevens. Totdat het zover is is de kans op een menselijke fout groter dan na doorvoering van die maatregelen. Beheersing van dit risico ligt in het bewust bezig zijn met persoonsgegevens en het melden van een datalek.

Vanuit de AP is informeel aangegeven dat in het eerste jaar vooral zal worden gekeken naar het benoemen van FG's en de aanpak een datalek. Met name klachten van burgers zullen serieuze aandacht van de AP krijgen. Daarnaast zal een organisatie moeten kunnen laten zien dat er serieus gewerkt wordt aan het compliant worden en blijven; boetes zullen daarom naar verwachting de eerste tijd niet snel aan de orde zijn, tenzij er sprake is van grove nalatigheid