Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

**Ministerie van Binnenlandse Zaken en Koninkrijksrelaties**

Turfmarkt 147
Den Haag
Postbus 20011
2500 EA Den Haag

**Kenmerk**
2020-0000610669

**Uw kenmerk**

| | |
|---|---|
| Datum | 21 oktober 2020 |
| Betreft | Beveiliging van privacygevoelige informatie in de BRP en andere basisregistraties |

In het Regeerakkoord[1] heeft het kabinet gemeld de gegevens van burgers in basisadministraties en andere privacygevoelige informatie versleuteld op te willen slaan.

In mijn brief van 4 november 2019[2] over de stand van zaken met betrekking tot de Basisregistratie Personen (BRP) heb ik gemeld dat ik in het kader van bovengenoemd punt uit het Regeerakkoord onderzoek heb laten uitvoeren naar de beveiliging van de BRP[3].

Daarnaast ben ik met de verantwoordelijken voor de andere basisregistraties in gesprek gegaan over hoe privacygevoelige informatie wordt beveiligd.

Naar aanleiding van de uitkomsten van het onderzoek en de gesprekken ben ik tot de conclusie gekomen dat (extra) versleuteling op dit moment niet de meest passende maatregel is voor het verbeteren van de bescherming van privacygevoelige informatie in de basisregistraties. Er valt meer winst te behalen door het nemen van andere maatregelen.

In het vervolg van deze brief rapporteer ik over de uitkomsten van het onderzoek en de gesprekken en licht daarbij de genomen en nog te nemen maatregelen toe.

*Resultaat onderzoek BRP en versleuteling*
De kwaliteit en de veiligheid van de gegevens in de BRP zijn essentieel voor het goed functioneren van onze samenleving. Ik heb de onderzoekers gevraagd de veiligheid van de BRP in brede zin te onderzoeken, met bijzondere aandacht voor de risico's die door de toepassing van versleuteling zouden kunnen worden verkleind. Het gaat dan bijvoorbeeld om misbruik van gegevens door ongeautoriseerde toegang of het uitlekken van gegevens.

[1] TK 2017/18 34700, nr. 34.
[2] Vergaderjaar 2019/2020 KST 27859-143.
[3] Het onderzoek is uitgevoerd door KPN.

Als bijlage stuur ik u de uitgebreide managementsamenvatting van het rapport waarin de onderzoekers hun bevindingen en aanbevelingen toelichten. Vanwege de vertrouwelijke informatie in het onderzoeksrapport wordt deze niet gepubliceerd. Op verzoek is het voor Kamerleden mogelijk om het rapport in te zien.

De onderzoekers concluderen, gelet op de risico-inventarisatie, de reeds bestaande beveiligingsmaatregelen en de kosten van aanvullende maatregelen, dat geen van de onderzochte vormen van aanvullend[4] versleutelen een zinvolle maatregel zou zijn. Dit volgt voornamelijk uit de functie van de BRP, waarbij grote aantallen gebruikers (> 600) en gemeenten de gegevens ontsleuteld moeten kunnen gebruiken in de eigen processen, waardoor het beveiligende effect van de versleuteling teniet wordt gedaan. Op basis van de onderzoeksresultaten heb ik besloten nu geen aanvullende versleuteling te gaan toepassen voor de gegevens in de BRP.

*Toelichting standpunt versleuteling basisregistratie*
Voor elk systeem dat gevoelige en/of persoonsgegevens omvat zijn maatregelen nodig die de beschikbaarheid, vertrouwelijkheid en integriteit van de informatie moeten borgen. Welke maatregelen de juiste zijn is afhankelijk van de situatie. Versleuteling kan op zichzelf niet alle facetten van beveiliging garanderen. Er zal altijd een combinatie van maatregelen nodig zijn die op diverse terreinen kunnen liggen. De mogelijke maatregelen zijn zeer divers. Naast technische maatregelen als versleuteling en autorisatie zijn bijvoorbeeld ook fysieke maatregelen als toegangscontrole tot locatie en apparatuur of organisatorische maatregelen als opleiding van personeel en inrichting van beheer mogelijk.

Veiligheid heeft continue aandacht nodig en daarom worden risico's regelmatig geïnventariseerd en beoordeeld. Het stelsel van maatregelen is continue aan verandering onderhevig door technische doorontwikkeling, nieuwe dreigingen en veranderende mogelijkheden. Op dit moment valt er meer winst te behalen door het nemen van andere maatregelen dan extra versleuteling. Voortschrijdend inzicht kan jaarlijks gebruikt worden om bijvoorbeeld ook de vragenlijst voor de zelfevaluatie BRP[5] bij te werken en zo een steeds beter inzicht te krijgen in de risico's voor burgers en overheid. In de toekomst kan blijken dat extra versleuteling wel een adequate maatregel kan worden.

[4] Het netwerk voor de berichtuitwisseling tussen partijen binnen het BRP-stelsel is reeds versleuteld.

[5] Met de jaarlijkse zelfevaluaties leggen gemeenten onder andere verantwoording af over de informatieveiligheid van de BRP aan de gemeenteraad en aan BZK.

*Activiteiten n.a.v. het onderzoek van de BRP*
De uitkomsten van het onderzoek en de aanbevelingen van de onderzoekers waren aanleiding het beveiligingsbeleid rond de BRP te heroverwegen. Hieronder schets ik de uitkomsten daarvan.

De hoofdaanbeveling, het centraliseren van de BRP, zal ik niet overnemen omdat de inrichting van de ICT-voorzieningen gebaseerd is op de decentraal belegde verantwoordelijkheden van onder andere gemeentes en BZK binnen het BRP-stelsel. De bestuurlijke inrichting van taken en verantwoordelijkheden is leidend voor de ondersteunende techniek. Er zijn geen voornemens om deze opzet ingrijpend te gaan veranderen. Gemeenten zijn en blijven verantwoordelijk voor de registratie en het bijhouden van gegevens van hun inwoners. Binnen dat uitgangspunt wordt gewerkt aan de veiligheid. Daarvoor zijn onder andere de zelfevaluaties ingericht waarmee iedere gemeente de staat van de beveiliging van het eigen gedeelte kent en zo nodig passende maatregelen kan nemen. Mijn aanpak voor de verbetering van de zelfevaluaties heb ik u in mijn Kamerbrief[6] van 2 december 2019 toegelicht. Ik zal de bevindingen van de onderzoekers meenemen in de verdere aanpak van de verbetering van de zelfevaluaties.

Daarnaast zal er bij de doorontwikkeling van de BRP aandacht besteed worden aan mogelijkheden om de privacy van burgers beter te borgen. Denk daarbij aan dataminimalisatie en meer bevragen bij de bron in plaats van het werken met kopieën. Ik informeer de Kamer daarover in een separate brief over de doorontwikkeling van de BRP.

Er zijn enkele bevindingen waarbij de Autoriteit Persoonsgegevens (AP) als toezichthouder een positieve bijdrage kan leveren aan de bewustwording over veiligheid. De bevindingen betreffen het protocolleren van gegevensverstrekkingen en het loggen van gebeurtenissen zodat het gebruik van de BRP gemonitord kan worden. De verplichting tot protocollering volgt uit de AVG. De AP kan vanuit haar rol als toezichthouder van de AVG gemeenten en gebruikers van de BRP wijzen op deze verplichting en de invulling daarvan controleren. Ik ga de AP informeren over deze bevindingen en vragen medewerking te verlenen om op deze punten gemeenten en gebruikers op hun verantwoordelijkheid aan te spreken.

De onderzoekers constateren dat gemeenten hulp kunnen gebruiken bij het verhogen van cyber-awareness en het omgaan met actuele dreigingen. Ik sluit wat betreft deze aanbeveling aan bij de ontwikkelingen bij de VNG. Daar wordt een centrale organisatie ingericht voor Gemeentelijke Gemeenschappelijke Infrastructuur Veilig (GGI-veilig). Tevens is er de informatiebeveiligingsdienst (IBD) van de VNG; die adviseert zowel preventief als in geval van spoed. Beide zijn aangesloten op de relevante kanalen en kunnen de gemeenten helpen, niet alleen voor de BRP maar ook voor en in samenhang met andere gemeentelijke systemen.

[6] Vergaderjaar 2019/2020 KST 27859-144.

Als laatste wil ik ingaan op de geconstateerde kwetsbaarheden die voortkomen uit verouderde techniek, met name in de GBA-berichtendienst. Het voornemen bestond al om deze te verbeteren, zoals ook al gemeld in de Kamerbrief van 4 november 2019 [7]. Ik kan hierbij melden dat deze werkzaamheden afgerond zijn en de berichtendienst gemoderniseerd en verbeterd is.

*Beleidslijn beveiliging privacygevoelige informatie basisregistraties*
Met de kennis uit het onderzoek naar de BRP is overleg gevoerd met de beleidsverantwoordelijke ministeries en verstrekkers van de andere basisregistraties die privacygevoelige informatie bevatten; de basisregistraties Inkomen, Voertuigen, WOZ, Handelsregister en Kadaster. Er is gesproken over hoe deze basisregistraties omgaan met beveiliging van privacygevoelige informatie. Versleuteling kan daarvoor een middel zijn, maar ook andere methodes zijn denkbaar om dat doel te bereiken.

Op basis van de reacties van de beleidsverantwoordelijke ministeries en de verstrekkers constateer ik dat deze basisregistraties handelen conform de overheidsbrede afspraak om de BIO (Baseline Informatiebeveiliging Overheid) te volgen en de verplichting om aan de AVG te voldoen.

Per 1 januari 2019 is de BIO van kracht. De BIO is van toepassing op alle overheidslagen (Rijk, provincies, gemeenten en waterschappen). In de BIO wordt gewerkt met basisbeveiligingsniveaus (BBN's). Aan de hand van een risicoanalyse wordt het beveiligingsniveau vastgesteld en worden passende maatregelen voorgeschreven. De BIO en de risicoanalyses zijn niet statisch. Inzichten uit bijvoorbeeld het jaarlijks Cybersecurity Beeld Nederland (CSBN) zijn input voor de door afzonderlijke organisaties uit te voeren risicoanalyses. En deze inzichten leveren ook een bijdrage aan de doorontwikkeling van de BIO.

Op privacygevoelige informatie met een verhoogd beveiligingsniveau is minimaal BBN2 van toepassing[8]. Gegevens die buiten het vertrouwde gebied worden verstuurd en vertrouwelijke gegevens op mobiele apparaten moeten conform BBN2 worden versleuteld. Alle verstrekkers hebben de ambitie om te voldoen aan de BIO, ook als deze (nog) niet op hen van toepassing is, zoals het geval is bij het zelfstandige bestuursorganen KVK die de basisregistratie Handelsregister beheert. Dit geldt ook voor RDW, die de basisregistratie Voertuigen beheert; RDW heeft al een gecertificeerd Informatiebeveiligingsmanagementsysteem (ISMS) dat gebaseerd is op dezelfde internationale standaarden als de BIO.

[7] Vergaderjaar 2019/2020 KST 27859-143.

[8] BBN2 is BasisBeveiligingsNiveau 2. Er zijn drie niveaus, waarbij BBN3 de zwaarste maatregelen vereist.

**Ministerie van Binnenlandse Zaken en Koninkrijksrelaties**

**Kenmerk**
2020-0000610669

Afdoende bescherming wordt door een complex van passende maatregelen geboden en is situationeel bepaald; versleuteling alleen is geen garantie voor veiligheid. Door het toepassen van de maatregelen behorende bij minimaal het BBN2 niveau worden (vertrouwelijke) gegevens in de basisregistraties op het juiste niveau beveiligd zodat privacygevoelige gegevens alleen door bevoegden kunnen worden ingezien en bewerkt. Hiermee wordt invulling gegeven aan alternatieve maatregelen met hetzelfde doel als het voornemen uit het Regeerakkoord, namelijk adequate beveiliging van de gegevens.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

drs. R.W. Knops