[redacted]

Datum 19 mei 2025
Onderwerp Besluit op uw Woo-verzoek
Behandeld door [redacted]
Ons kenmerk Z25-2338 / D25-15204
Uw kenmerk -
Bijlagen 8

Geachte verzoeker,

Op 6 april 2025 heeft u bij Staatsbosbeheer een verzoek ingediend als bedoeld in artikel 4.1, eerste lid, van de Wet open overheid (hierna: Woo). Uw verzoek gaat – kort gezegd – over de omgang met persoonsgegevens door Staatsbosbeheer.

Met deze brief besluit ik op uw gehele Woo-verzoek. Aanvankelijk heeft de behandelaar met u afgesproken om met deelbesluiten te werken, maar dit is in de praktijk niet nodig gebleken. Alle documenten die onder de reikwijdte van uw verzoek vallen, zijn dus tegelijk verzameld en beoordeeld. Deze ontvangt u (geanonimiseerd) bij dit besluit.

Hieronder leest u mijn besluit en hoe ik hiertoe gekomen ben. Ook geef ik u meer informatie over wat u kunt doen als u het niet eens bent met dit besluit.

Besluit

Ik besluit tegemoet te komen aan uw verzoek en 7 documenten (deels) openbaar te maken. In de bijlage bij dit besluit treft u de documenten en een overzicht aan. De paginanummers op het overzicht komen overeen met de paginanummers op de documenten.

In de bijgevoegde stukken heb ik bepaalde gegevens (deels) onleesbaar gemaakt. Voor de motivering verwijs ik u naar de overwegingen. Per onleesbaar gemaakt onderdeel is zichtbaar op basis waarvan de informatie niet openbaar wordt gemaakt.

De manier van openbaar maken

Ik stuur de documenten gelijk bij dit besluit mee, omdat ik niet verwacht dat er bezwaar is tegen het openbaar maken van de documenten.

Naast dat ik u dit besluit en de bijlagen toestuur, zal ik deze ook in geanonimiseerde vorm publiceren op de website van Staatsbosbeheer, zodat deze voor iedereen toegankelijk worden.

Uw Woo-verzoek

In uw verzoek vraagt u om documenten openbaar te maken, namelijk *'informatie over de omgang met persoonsgegevens door Staatsbosbeheer, in het bijzonder met betrekking tot het noteren van het Burgerservicenummer (BSN) bij handhavingssituaties.'* U schrijf dat u specifiek verzoekt om de volgende informatie en documenten:

1. Beleidsdocumenten, protocollen of richtlijnen waarin is vastgelegd hoe Staatsbosbeheer omgaat met persoonsgegevens van burgers bij handhaving of controle.
2. Informatie over het gebruik en vastleggen van het BSN in dergelijke situaties.
3. Interne richtlijnen over het opschrijven van persoonsgegevens op papier (zoals naam, adres, BSN) door boa's of andere handhavers.
4. Eventuele overeenkomsten of verwerkersafspraken met derde partijen die toegang hebben tot deze gegevens.
5. Eventuele meldingen van datalekken of klachten met betrekking tot de omgang met persoonsgegevens door Staatsbosbeheer in de afgelopen 5 jaar.

Wat aan dit besluit vooraf is gegaan

Hieronder geef ik in het kort aan wat er is gebeurd nadat u uw verzoek heeft ingediend bij Staatsbosbeheer.

Op 10 april 2025 heb ik de ontvangst van uw verzoek bevestigd. In deze brief heb ik u tevens mijn lezing van uw verzoek gegeven, namelijk dat punt 5 van uw verzoek zich tevens enkel richt op persoonsgegevens *uit handhavingssituaties*. Ik heb aangegeven dat ik zonder tijdig tegenbericht uitga van deze lezing.

Diezelfde dag heeft u per e-mail gereageerd dat deze lezing niet juist is. U heeft aangegeven dat punt 5 zich niet enkel beperkt tot handhavingssituaties. Zodoende ben ik aangaande punt 5 op zoek gegaan naar documenten die zien op *alle* 'eventuele meldingen van datalekken of klachten met betrekking tot de omgang met persoonsgegevens door Staatsbosbeheer in de afgelopen 5 jaar'.

Op 1 mei 2025 heb ik de beslissing op uw verzoek, op grond van artikel 4.4 lid 2 van de Woo, met twee weken uitgesteld.

Op 8 mei 2025 heb ik een derde-belanghebbende om een zienswijze gevraagd, volgens art. 4:8 van de Algemene wet bestuursrecht (Awb). Ik heb u hiervan op de hoogte gesteld en u laten weten dat de termijn niet verder liep, totdat de zienswijze kenbaar was gemaakt. De termijn is hierdoor één dag opgeschort geweest. De derde-belanghebbende heeft aangegeven geen bezwaren te hebben tegen de openbaarmaking.

Resultaten onderzoek

Ik heb uitgebreid onderzoek gedaan of Staatsbosbeheer de documenten heeft waarop uw informatieverzoek betrekking heeft. Ik heb hiervoor het (digitaal) archief, de systemen en de betrokken collega's geraadpleegd.

Het moment waarop u uw verzoek heeft gedaan, heeft gevolgen voor naar welke documenten zijn gezocht. Een Woo-verzoek kan niet gaan over documenten die na het opsturen van uw verzoek zijn geschreven.[1] Dit houdt in dat documenten die later zijn gemaakt dan de datum van uw verzoek, 6 april 2025, niet zijn meegenomen bij de behandeling van uw verzoek.

[1] ABRvS 4 maart 2015, ECLI:NL:RVS:2015:623.

Een deel van de informatie die u vraagt in punt 5 van uw verzoek is reeds openbaar gemaakt bij een eerder besluit op een Woo-verzoek.[2] Dat verzoek ging over procedures en beleid ten aanzien van datalekken. In document 1 bij dat besluit, genaamd *'overzicht van inbreuken jan 2020 t/m dec 2021'*, is de door u gevraagde informatie aangaande meldingen van datalekken of klachten met betrekking tot de omgang met persoonsgegevens voor de jaren 2020 en 2021 al openbaar. De Woo is niet van toepassing op documenten die al openbaar zijn. Het besluit met de documenten is te raadplegen via: https://www.staatsbosbeheer.nl/-/media/19-wob/20240510-woo-besluit-vermeende-datalekken-2020-tm-2021.pdf.

Ik ben zodoende voor dit besluit op zoek gegaan naar de documenten aangaande de punten uit uw verzoek die nog niet openbaar zijn, namelijk punt 1 t/m 4 en de informatie over 1 januari 2022 t/m 5 april 2025 aangaande punt 5.

Ik heb 7 documenten gevonden.

Overwegingen

Het uitgangspunt van de Woo is dat overheidsinformatie zoveel mogelijk openbaar wordt gemaakt als daar om wordt verzocht. Hierop bestaan enkele uitzonderingen. De voor dit besluit relevante uitzonderingsgronden komen hieronder aan bod.

De eerbiediging van de persoonlijke levenssfeer, art. 5.1, lid 2 sub e, Woo

De documenten die vallen onder uw verzoek bevatten persoonsgegevens. Deze persoonsgegevens worden op grond van artikel 5.1, tweede lid, aanhef en sub e, Woo niet openbaargemaakt als het belang daarvan niet opweegt tegen het belang van de bescherming van de persoonlijke levenssfeer. In de documenten staan bijvoorbeeld namen en handtekeningen van personen die niet met hun functie in de openbaarheid treden. Van openbaarmaking hiervan wordt, in lijn met vaste rechtspraak, meestal afgezien.[3] Namen van personen die in hun functie in de openbaarheid treden, worden wel openbaar gemaakt.

Het goed functioneren van Staatsbosbeheer art. 5.1, lid 2 sub i, Woo

In enkele documenten heb ik de namen aangetroffen van systemen die Staatsbosbeheer gebruikt. Het openbaar maken van de namen van deze systemen kan het voor anderen gemakkelijker maken om zich hiertoe gericht toegang te verschaffen. Dit geldt temeer wanneer het gaat om systemen die door vrijwel alle medewerkers worden gebruikt. Om te voorkomen dat kwaadwillende personen (zoals hackers) deze informatie inzetten om in te breken in deze systemen, maak ik deze informatie niet openbaar.

Daarnaast heb ik in één van de documenten de locatie van bepaalde bestanden op de harde schijf van een computer – een zogenoemde '*pad*'- aangetroffen. Deze locatie maak ik tevens niet openbaar, vanuit dezelfde veiligheidsoverwegingen als het niet openbaar maken van de systeemnamen.

Rechtsmiddelen

Indien u het niet eens bent met dit besluit, kunt u binnen zes weken na verzending van dit besluit schriftelijk bezwaar maken. Ook een andere belanghebbende kan tegen dit besluit bezwaar maken. Het bezwaarschrift kan worden gestuurd aan de Directeur Staatsbosbeheer, Postbus 2, 3800 AA Amersfoort. U kan uw bezwaarschrift ook per e-mail versturen naar info@staatsbosbeheer.nl. U wordt verzocht een afschrift van dit besluit bij het bezwaarschrift te voegen.

Een bezwaarschrift moet zijn ondertekend en bevat tenminste:

[2] Met zaaknummer Z24-2844.
[3] ABRvS 31 januari 2018, ECLI:NL:RVS:2018:321.

- uw naam en adres;
- een datum;
- een omschrijving van het besluit waartegen het bezwaar is gericht;
- de redenen waarom u het niet eens bent met het besluit.

Het niet voldoen aan deze eisen kan leiden tot niet-ontvankelijkheid van het bezwaarschrift. Dat betekent dat uw bezwaar niet inhoudelijk wordt behandeld.

Als u nog vragen heeft, dan kunt u contact opnemen met [redacted] of Woo@staatsbosbeheer.nl.

Met vriendelijke groet,

de [redacted] sbeheer, namens deze,

in
(w [redacted] ur Terreinbeheer & Ontwikkeling

Documentenoverzicht Woo-besluit - Zaaknummer: *Z25-2338*

Vanaf pagina	Naam / Kernwoorden	d.d. document	Openbaar gemaakt?
	Punt 1 t/m 4 van uw verzoek:		
1	1. Werkvoorschrift Omgaan met WPG gegevens	1 november 2024	Ja, geheel
7	2. Convenant Samenwerkingsverband uitwisseling Politiegegevens BRS	21 september 2020	Ja, deels
26	3. Annex bij Samenwerkingsverband - Verwerkersovereenkomst	21 september 2020	Ja, deels
	Punt 5 van uw verzoek:		
36	4. Inbreuken in verband met persoonsgegevens overzicht 2022	2022	Ja, deels
41	5. Inbreuken in verband met persoonsgegevens overzicht 2023	2023	Ja, deels
45	6. Inbreuken in verband met persoonsgegevens overzicht 2024	2024	Ja, deels
52	7. Inbreuken in verband met persoonsgegevens overzicht 2025	2025	Ja, geheel

WERKVOORSCHRIFT

Naam	Omgaan met WPG gegevens
Proceseigenaar	Directie Bestuur & Strategie
Uitgiftedatum	1 november 2024
Versie	2.1

1) Doel van het werkvoorschrift

Dit werkvoorschrift beschrijft hoe omgegaan moet worden met politiegegevens, die in een bestand zijn opgenomen of die bestemd zijn daarin te worden opgenomen, door de buitengewoon opsporingsambtenaren (boa´s) van Staatsbosbeheer.

Dit werkvoorschrift heeft tot doel alle handelingen met politiegegevens te laten plaatsvinden conform de regels van uit de Wet politiegegevens (Wpg) en de bijbehorende besluiten.
Het gaat dan vooral om het verzamelen, delen, veilig opslaan en het bewaren van deze gegevens.

Verwerkingsverantwoordelijke is volgens artikel 1 onder c van het Besluit politiegegevens buitengewoon opsporingsambtenaar de werkgever van de buitengewoon opsporingsambtenaren, dus Staatsbosbeheer.

De verwerkingsverantwoordelijke dient periodiek (jaarlijks) te controleren of er op juiste wijze uitveoring wordt gegeven aan de regels van de Wpg. Er zal jaarlijks een interne audit plaatsvinden om na te gaan of er op een juiste wijze wordt om gegaan met het verwerken van politiegegevens door Staatsbosbeheer. Daarnaast zal er 1x in de vier jaar een externe audit plaatsvinden.
Een afschrift van de resultaten van de externe audit dienen aan de Autoriteit Persoonsgegevens gezonden te worden.

2) Begrippen

Persoonsgegevens:

Elk gegeven betreffende een identificeerbaar of geïdentificeerde natuurlijke persoon. Het gaat dus om NAW gegevens, foto´s, filmopname, kenteken of telefoonnummer e.d.

Politiegegevens:

Persoonsgegevens die worden verwerkt in het kader van de uitoefening van de politietaak.

Bijzondere persoonsgegevens:

Onder bijzondere persoonsgegevens worden onder andere ras, godsdienst of gezondheid verstaan.

Ter beschikking stellen:

Het delen van politiegegevens met personen en instanties die deze gegevens verwerken volgens de regels van de Wpg. De zogenaamde “free flow of information” zoals beschreven in artikel 15 van de Wpg. In principe worden politiegegevens gedeeld met andere handhavers voor zover zij deze nodig hebben voor de uitoefening van hun taak.

Verstrekken:

Het delen van politiegegevens met andere personen en instanties dan degene die bij “ter beschikking stellen” in art. 1 onder e Wpg zijn genoemd. Dus met andere partijen dan de collega handhavers (boa´s en politie e.d.). Denk aan een gemeente of de eigen organisatie voor schadeverhaal.

WERKVOORSCHRIFT

Naam	Omgaan met WPG gegevens
Proceseigenaar	Directie Bestuur & Strategie
Uitgiftedatum	1 november 2024
Versie	2.1

Verwerken

Elke bewerking van politiegegevens zoals verzamelen, opschrijven, opnemen, filmen, fotograferen, registreren, aanpassen en zelfs verwijderen.

3) Werkvoorschrift

1. Verzamelen gegevens

Het boa-registratiesysteem (BRS) voldoet aan alle eisen van de Wpg. Het is daarom ook wenselijk om politiegegevens rechtstreeks in BRS te zetten. Dit voorkomt onnodige risico´s en zelfs mogelijke datalekken. Verzamel je toch politiegegevens op een andere wijze dan dient de hieronder weergegeven richtlijn gevolgd te worden.

Opschrijven in notitieboekje	a) Direct, doch uiterlijk na 24 uur, na overnemen in BRS verwijderen uit het boekje. b) Blaadje uit boekje verwijderen en vernietigen (versnipperen).
Uitschrijven papieren combibon	a) “Geeltje” aan verdachte uitreiken. b) Origineel na overname gegevens in BRS vernietigen (verbranden of versnipperen).
Opnemen beelden met camera: a. Bodycam b. Wildcamera c. Drone d. Dashcam e. Telefoon	a) Volgen van het werkvoorschrift “Gebruik bodycam”. b) Als er sprake is van stelselmatige observatie alleen met schriftelijke toestemming van de OvJ (126 Sv), zodat duidelijk is dat de beelden als ondersteunend bewijs zijn toegestaan. In de andere gevallen valt het gebruik onder de reguliere taak. Het gaat dan om een koststondig gebruik met een beperkte inbreuk op de privacy. c) Niet gebruiken voor vastleggen personen / politiegegevens. Nog niet geregeld. d) Te gebruiken voor vastleggen personen / politiegegevens. e) Opname z.s.m. uploaden naar BRS. Daarna direct verwijderen van de telefoon.
Maken foto´s van identiteitsbewijs	Niet toegestaan (disproportioneel). Kan alleen met behulp van de KopieID-app van het Ministerie van BZK. Na het opstellen van het bijbehorende proces-verbaal gegevens direct verwijderen.
Proces-verbaal op [redacted] of in de Teamsgroep Boa	Permanent opslaan niet toegestaan. Is weliswaar alleen toegankelijk voor boa´s maar niet iedereen heeft de betreffende gegevens nodig voor de uitvoering van zijn taak.

WERKVOORSCHRIFT

Naam	Omgaan met WPG gegevens
Proceseigenaar	Directie Bestuur & Strategie
Uitgiftedatum	1 november 2024
Versie	2.1

	Er mag wel een voorbeeld pv of imprimé worden geplaatst. Dan dienen wel de persoonsgegevens en locatiegegevens verwijderd te zijn. Ook kan een proces-verbaal waar nog aan gewerkt wordt tijdens de ontwikkeling hier worden opgeslagen. Na afronding dan wel verwijderen.

Landelijke boa-coördinatie controleert 1x per kwartaal:
- K-schijf (zolang die nog wordt gebruikt);
- Teamsgroep BOA;
- Zepcam;
- Privacy dashboard BRS;

Op (on)terechte opslag van politiegegevens of het raadplegen ervan.

Verlies of onbevoegde inzage van het notitieboekje, filmbeelden, foto´s, BRS of een proces-verbaal met daarin politiegegevens direct melden bij de functionaris gegevensbescherming (fg@staatsbosbeheer.nl).

Er vindt geen verwerking van bijzondere categorieën van persoonsgegevens plaats, tenzij:
- dat onvermijdelijk is voor het doel van de verwerking;
- dit in aanvulling is op de verwerking van andere politiegegevens betreffende de persoon;
- de gegevens afdoende zijn beveiligd.

Indien de hierboven genoemde uitzondering aan de orde is vindt registratie plaats in overleg met de landelijke boa-coördinatie. Zij registreren de wijze van verwerking en het doel.

2. Delen van gegevens

Verstrekken van gegevens altijd via BRS. Als gegevens via BRS worden verstrekt dan wordt deze verwerking gelogd. Er is dus altijd terug te vinden aan wie de gegevens zijn verstrekt.
Een ieder aan wie politiegegevens ter besschikking zijn gesteld of aan wie politiegegevens zijn verstrekt is verplicht tot geheimhouding daarvan, behoudens de uitzonderingen die in de wet zijn genoemd.
Verstrekken of delen van gegevens buiten BRS in principe niet. Als het echt niet anders kan dan goed verifiëeren bij wie de gegevens terecht komen.

Delen via mail	a) Weet wie deze mail kan lezen b) Weet zeker dat deze persoon over de gegevens mag beschikken c) Weet waarvoor de gegevens worden gebruikt (doelbinding).
Delen via whatsappgroep of BBM	a) Weet wie er allemaal in de whatsappgroep zitten

	b) Weet zeker dat al deze personen over de gegevens mogen beschikken c) Weet waarvoor de gegevens worden gebruikt (doelbinding). d) Bij voorkeur 1 op 1 delen zodat bovenstaande vragen beter te beantwoorden zijn.
Delen op papier	a) Weet wie deze gegevens kan lezen b) Weet zeker dat deze persoon of personen over de gegevens mogen beschikken c) Weet waarvoor de gegevens worden gebruikt (doelbinding).
Delen telefonisch	a) Weet wie je aan de lijn hebt. b) Weet zeker dat deze persoon over de gegevens mag beschikken. c) Weet waarvoor de gegevens worden gebruikt (doelbinding).

3. Rechten betrokkenen

Personen van wie politiegegevens zijn vastgelegd hebben op grond van de Wpg een aantal rechten. Via de website van Staatsbosbeheer (www.staatsbosbeheer.nl/privacy) kunnen zij zien hoe zij aan hun rechten invulling kunnen geven.
Dit kunnen zij vinden in de privacyverklaring en op de pagina over boa. Hier staan een aantal onderwerpen op voor mensen die een bekeuring of officiële waarschuwing hebben gekregen. Zij kunnen ook rechtstreeks naar www.privacyvragenbrs.nl.
Wijs de mensen hier op.

4. Verwijderen en/of vernietigen van gegevens

Poltiegegevens vallen onder de Wpg. Deze wet kent ook termijnen voor het bewaren van gegevens. Hierbij wordt wel onderscheid gemaakt tussen verwijderen en vernietingen. Daarnaast is het van belang of de gegevens worden verwerkt onder het regime van artikel 8 of van artikel 9. Hier hangen verschillende bewaartermijnen aan. Onderstaand het verschil tussen verwijderen en vernietigen en een opsomming van enkele criteria. Voor een volledige opsomming: raadpleeg de genoemde artikelen.

Verwijderen
In de Wpg wordt met verwijderen bedoeld het buiten de operationele verwerking plaatsen van politiegegevens. Verwijderen is dus een privacybevorderende maatregel, namelijk door het beperken van de toegang. Verwijderde gegevens zijn wel beschikbaar, maar alleen voor functioneel of technisch beheerders, of medewerkers die zich bijvoorbeeld bezig houden met klachtafhandeling of het hernieuwd verwerken.

Vernietigen
Onder vernietigen (Wpg) verstaan we het onherstelbaar wissen van persoonsgegevens. In de AVG wordt het begrip wissen gehanteerd. Wissen en vernietigen hebben totale werking, ook naar registraties in het verleden.

Artikel 8 gegevens verwijderen
Een jaar na de datum van de eerste verwerking (artikel 8, lid 6 Wpg) dienen de gegevens verwijderd te worden. Of zoveel eerder indien blijkt dat gegevens niet meer nodig zijn voor het doel waar ze oorspronkelijk voor verwerkt werden (artikel 8, lid 6 en artikel 4 lid 2 Wpg).

Artikel 8 gegevens vernietigen
Verwijderde gegevens worden gedurende vijf jaar bewaard en vervolgens vernietigd (artikel 14, lid1 Wpg).

Artikel 9 gegevens verwijderen
- Zodra de gegevens niet meer noodzakelijk zijn voor het doel van het onderzoek.
- Of na verloop van een periode van maximaal een half jaar waarin ze verwerkt worden om te bezien of ze aanleiding geven tot een nieuw onderzoek (‘herbruikbare informatie’).
- Als de verdachte of veroordeelde is overleden wordt het dossier in overleg met de Officier van Justitie opgelegd en wordt de verwerking beëindigd.

Artikel 9 gegevens vernietigen
Verwijderde gegevens worden gedurende 5 jaar bewaard en vervolgens vernietigd (artikel 14, lid 1 Wpg).

5. Relevante websites en telefoonnummers.

www.Staatsbosbeheer.nl - privacyverklaring
- Boa pagina op de website

www.privacyvragenbrs.nl - rechten van betrokkenen

Toelichting grondslagen

In dit document kunt u secties vinden die onleesbaar zijn gemaakt. Deze informatie is achterwege gelaten op basis van de Wet open overheid (Woo). De letter die hierbij is vermeld correspondeert met de bijbehorende grondslag in onderstaand overzicht.

N Art. 5.1 lid 2 sub i

Het belang van de openbaarmaking van deze informatie weegt niet op tegen het belang van het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen

BRS

Kennedy Van der Laan

Convenant Samenwerkingsverband uitwisseling Politiegegevens BRS

Inleiding

In het Boa Registratie Systeem (BRS) worden handhavingsactiviteiten door buitengewoon opsporingsambtenaren (Boa's) geregistreerd. Registratie in BRS vindt plaats ten behoeve van de Boa zelf, de werkgever, politie, justitie en overige opsporingsdiensten en ten behoeve van de uitwisseling tussen Boa's onderling binnen de bevoegdheden van het domein en buiten het domein voor zover dat past binnen de wettelijke opsporingsbevoegdheden van de Boa. Dit Convenant Samenwerkingsverband uitwisseling Politiegegevens BRS (hierna: "Convenant") ziet op de wijze waarop Politiegegevens worden verwerkt in het kader van het BRS. De Partijen bij het Convenant hebben allen als werkgever, als samenwerkingsverband van werkgevers of als coördinerende organisatie van Boa's een licentieovereenkomst afgesloten met NatuurNetwerk BV (hierna 'NatuurNetwerk'), waardoor de Boa's die werkzaam zijn voor of ten behoeve van de Partijen van het BRS gebruik kunnen maken.

Een eerste versie van dit Convenant is in 2014 ontwikkeld in overleg met het Ministerie van Veiligheid en Justitie en het College bescherming persoonsgegevens. Destijds voorzag het convenant in de behoefte om afspraken vast te leggen over wie verantwoordelijke is in de zin van de Wet bescherming persoonsgegevens (Wbp) voor het BRS en over de wijze waarop Persoonsgegevens in het BRS worden verwerkt. Aangenomen werd dat het convenant zou voorzien in een tijdelijke behoefte, in afwachting van nog te ontwikkelen wetgeving waarin de verantwoordelijkheid voor de verwerking van Persoonsgegevens in het BRS op structurele wijze wordt belegd.

Doordat de Wbp met ingang van 25 mei 2018 werd ingetrokken is er per 25 mei een aangepaste versie van dit Convenant van kracht geworden met daarin aanpassingen aan de toen geldende situatie.[1]

Met ingang van 9 maart 2019 is de verwerking van Persoonsgegevens door Boa's onder de Wet politiegegevens (hierna 'Wpg'), meer specifiek onder het Besluit politiegegevens buitengewone opsporingsambtenaren (hierna 'het Besluit') gebracht. Als gevolg daarvan worden de Persoonsgegevens die Boa's verwerken in het kader van hun opsporingstaken aangemerkt als Politiegegevens. Op basis hiervan is het voorliggende convenant opnieuw aangepast naar de laatste stand van zaken.

In het voorliggend Convenant Samenwerkingsverband uitwisseling Politiegegevens BRS zijn afspraken vastgelegd tussen de werkgevers van de Boa's, die in het Besluit zijn aangewezen als Verwerkingsverantwoordelijken, en samenwerkingsverbanden van werkgevers van de Boa's. Het gaat

[1] Daarvoor is in de plaats getreden de Algemene verordening gegevensbescherming en de Uitvoeringswet algemene verordening gegevensbescherming.

om gezamenlijke besluitvorming over de inrichting van het BRS en over de wijze waarop Politiegegevens in het kader van het BRS worden verwerkt en uitgewisseld.

Toelichting: Partijen zijn de Boa-werkgevers, de samenwerkingsverbanden van werkgevers (zoals regionale uitvoeringsdiensten) alsmede de coördinerende organisaties waarvoor of ten behoeve waarvan Boa's werkzaam zijn, die een licentieovereenkomst hebben gesloten met NatuurNetwerk. De Boa's in dienst van of werkzaam ten behoeve van Partijen mogen gebruik maken van het BRS. Alle Partijen en hun contactpersonen worden genoemd in het BRS.

Partijen overwegen daarbij als volgt:

1. Voor de uitvoering van de primaire taken van de Boa's binnen hun wettelijke opsporingsbevoegdheden is het noodzakelijk dat zij Politiegegevens verwerken, waaronder in ieder geval begrepen het verzamelen, vastleggen en uitwisselen met bevoegde instanties en Boa's. Door middel van dit Convenant wordt een Samenwerkingsverband uitwisseling Politiegegevens BRS (hierna: "SupBRS") gecreëerd;
2. Partijen wensen onderling afspraken te maken over de wijze waarop het BRS wordt ingericht, over de wijze waarop Politiegegevens in het kader van het BRS worden verwerkt en uitgewisseld en Boa's elkaar kunnen waarschuwen in geval van noodsituaties, de inrichting van één aanspreekpunt voor de Betrokkenen van wie gegevens in het BRS worden verwerkt, de manier waarop Betrokkenen hun rechten kunnen uitoefenen en de afspraken die worden gemaakt met de Verwerker NatuurNetwerk;
3. Partijen zijn ieder Verwerkingsverantwoordelijke voor de eigen gegevensverwerkingen in de compartimenten van het BRS door de Boa's die bij hen in dienst zijn of ten behoeve van hen werkzaam zijn;
4. Partijen zijn zich bewust van de grenzen die de toepasselijke wet- en regelgeving op het gebied van de bescherming van Politiegegevens en Persoonsgegevens stelt aan het vastleggen en uitwisselen van die gegevens;
5. Partijen verbinden zich ten opzichte van elkaar om in overeenstemming met hetgeen in dit Convenant is bepaald, te handelen en op de door hen afgesproken wijze Politiegegevens in het BRS te laten verwerken en uitwisselen, Boa's in staat te stellen via beveiligde applicaties te communiceren en meldingen te doen in geval van noodsituaties, een aanspreekpunt in te richten waar de Betrokkene, wiens gegevens worden verwerkt, terecht kan en gezamenlijke afspraken te maken met de Verwerker NatuurNetwerk.

Toelichting: de wet- en regelgeving op het gebied van bescherming van Politiegegevens stelt grenzen en eisen aan de mogelijkheden om Politiegegevens uit te wisselen of te delen (op structurele basis of incidenteel). Daarom moet helder zijn welke bepalingen ten aanzien van het samenwerkingsverband uitwisseling Politiegegevens BRS van toepassing zijn. De Wpg en het Besluit stellen het algemene kader voor de verwerking van Politiegegevens door Boa's in het kader van hun wettelijke opsporingsbevoegdheden. Het Convenant geeft een nadere uitwerking aan deze algemene bepalingen. In het

Convenant worden afspraken gemaakt over de wijze waarop Politiegegevens worden verwerkt in het BRS, over wie toegang heeft tot gegevens in het BRS en op welke wijze gegevens worden uitgewisseld. De toegang tot de Politiegegevens die in het BRS worden verwerkt wordt door middel van technische en organisatorische beveiligingsmaatregelen (waaronder autorisaties) beperkt. Daarnaast stelt ook de wet- en regelgeving op het gebied van bescherming van Persoonsgegevens (de Algemene verordening gegevensbescherming en de Uitvoeringswet AVG) grenzen aan de mogelijkheden om in het kader van BRS Persoonsgegevens (anders dan Politiegegevens) te verwerken. Het gaat dan bijvoorbeeld om verwerking van Persoonsgegevens van Boa's en om de inrichting van de verwerking van meldingen van Boa's in noodsituaties.

Partijen komen het volgende overeen:

DEFINITIES

1. In dit Convenant wordt verstaan onder:

1.1 **Boa**: buitengewoon opsporingsambtenaar, een functionaris die uit hoofde van zijn taak, in ondergeschiktheid aan het bevoegde gezag, in overeenstemming met de geldende rechtsregels en met behulp van de hem daartoe beschikbaar gestelde bevoegdheden en middelen, zorg draagt voor de opsporing van strafbare feiten alsmede de voorbereiding van de eventuele vervolging van die feiten en die in het bezit is van een geldige akte of aanwijzing van opsporingsbevoegdheid als bedoeld in artikel 142, tweede lid, van het Wetboek van Strafvordering;

1.2 **Boa Registratie Systeem of BRS**: door NatuurNetwerk ontwikkelde (technische) voorzieningen ten behoeve van uitvoering van opsporingstaken door Boa's en ten behoeve van uitvoering van verantwoordelijkheden van werkgevers van Boa's, waaronder in ieder geval begrepen een systeem voor de registratie van handhavingshandelingen, waarnemingen, waarschuwingen en maatregelen door Boa's alsmede applicaties voor communicatie tussen Boa's en operationele aansturing van Boa's;

1.3 **Partij**: Partij bij dit Convenant en organisatie of instantie die een of meer Boa's in dienst heeft dan wel ten behoeve waarvan Boa's werkzaamheden verrichten en die beschikt over een door NatuurNetwerk uitgegeven licentie voor het gebruik van het BRS;

1.4 **Persoonsgegeven**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon;

1.5 **Politiegegeven**: elk Persoonsgegeven dat wordt verwerkt in het kader van de uitoefening van de opsporingstaak door een Boa;

1.6 **Betrokkene**: natuurlijke persoon op wie een Persoonsgegeven betrekking heeft;

1.7 **Verwerking**: elke bewerking of elk geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd op geautomatiseerde wijze, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, afschermen of vernietigen van Persoonsgegevens;

1.8 **Verwerkingsverantwoordelijke**: de werkgever van de Boa, zoals bepaald in artikel 1, onderdeel h, van het Besluit buitengewoon opsporingsambtenaar dan wel de gemeenschappelijke Verwerkingsverantwoordelijke die daartoe door de betrokken Verwerkingsverantwoordelijken is aangewezen in het kader van een gemeenschappelijke verwerking;

1.9 **Verwerker**: degene die ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt, zonder aan diens rechtstreeks gezag onderworpen te zijn.

1.10 **Technische Gebruikers Groep of TGG**: groep van werkgevers van Boa's dan wel coördinerende organisaties die een licentie hebben op het BRS. Het werkveld is ingedeeld in secties en elke sectie heeft haar eigen Technische Gebruikersgroep (TGG) in BRS. Voor de werking van TGG is een reglement opgesteld. Dit TGG Reglement is beschikbaar in BRS voor de werkgever contactpersonen.

1.11 **Regiegroep**: overleggroep van afgevaardigden van de Technische Gebruikers Groepen.

RECHTEN EN VERPLICHTINGEN

2 Verantwoordelijkheid voor de verwerking

2.1 Gezamenlijke inrichting en verantwoordelijkheid BRS

In het SupBRS nemen de licentiehouders als Verwerkingsverantwoordelijken voor de verwerking van Politiegegevens in het BRS gezamenlijk bepalende besluiten over de inrichting van het BRS. In het SupBRS stellen zij de doeleinden van de gegevensverwerking in het BRS vast en bepalen zij op welke wijze van het BRS gebruik kan worden gemaakt.

De Partijen bij het SupBRS zijn ieder afzonderlijk verantwoordelijk voor het instrueren van de Boa's die ten behoeve van hen of in hun dienst werkzaam zijn.

Toelichting: In het SupBRS nemen de licentiehouders gezamenlijk besluiten over het BRS. De licentiehouders zijn enerzijds de (samenwerkingsverbanden van) werkgevers van de Boa's die Verwerkingsverantwoordelijke zijn voor de gegevensverwerking door de Boa, anderzijds vertegenwoordigers van (samenwerkingsverbanden van) werkgevers van de Boa's die gemachtigd zijn om namens de (samenwerkingsverbanden van) werkgevers als licentiehouder deel te nemen in BRS en de Boa's aan te sturen die ten behoeve van hen werkzaam zijn. Het gaat hier onder meer om de wijze waarop gegevens in het BRS kunnen worden geraadpleegd door de verschillende individuele Boa's, alsmede de wijze van afscherming en uitwisseling van de gegevens. Het gaat aldus om de inrichting van het systeem voor de verwerking van Politiegegevens in het BRS en inrichting van communicatievoorzieningen tussen Boa's onderling alsmede voor operationele aansturing van Boa's. Naast de besluitvorming in het SupBRS, hebben de afzonderlijke Partijen ook ieder een eigen verantwoordelijkheid voor dat eigen "stukje" van het BRS waarin de Boa's die in hun dienst of ten behoeve van hen werkzaam zijn Politiegegevens verwerken. Het gaat dan om Politiegegevens die door de individuele Boa's in het systeem worden ingevoerd. Zie ook onder 2.2. Een eigen verantwoordelijkheid bestaat ook voor zover werkgevers gebruik maken van de voorzieningen voor operationele aansturing van de Boa's.

In het SupBRS bepalen Partijen gezamenlijk:

a) de doeleinden van gegevensverwerking alsmede het technisch en functioneel beheer van het BRS;
b) de inrichting van toegang tot basisregistraties binnen de wettelijke bevoegdheden van Boa's;
c) de controle op de toegang tot gegevensverwerkingen in het BRS aan de hand van autorisatie voor het systeem en controle op de logging van het gebruik;
d) de procedure voor het in ontvangst nemen van verzoeken van Betrokkenen ten aanzien van hen betreffende verwerkingen van Politiegegevens op grond van de artikelen 12 en volgende en doorsluizen van een verzoek aan een Verwerkingsverantwoordelijke;
e) de procedure voor het in ontvangst nemen en afhandelen van verzoeken tot verstrekking van anonieme rapportages op basis van in BRS verwerkte gegevens alsmede verstrekking van Politiegegevens voor wetenschappelijke en statistische doeleinden;
f) het treffen van passende technische en organisatorische maatregelen om de Politiegegevens in het BRS te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking;
g) de uitbesteding van de uitvoering van het technisch en functioneel beheer van het BRS alsmede de onder b tot en met f genoemde activiteiten aan NatuurNetwerk als Verwerker.

Toelichting: Onder functioneel beheer valt bijvoorbeeld het toekennen van autorisaties. Onder technisch beheer valt bijvoorbeeld het onderhouden van de technische infrastructuur, het beschikbaar stellen van verwerkings- en opslagcapaciteit. In het verlengde van de besluitvorming over het functioneel en technisch beheer beslist het SupBRS over de technische en organisatorische beveiligingsmaatregelen, het systeem voor autorisaties voor toegang tot Politiegegeven en voor (structurele en incidentele) verstrekking van Politiegegevens, de modelverklaring voor verlenen van autorisatie door een Partij aan een niet-Boa en over de inrichting van beveiligde applicaties voor communicatie tussen Boa's, waaronder ook noodmeldingen (locatiegegevens) door Boa's. Verder berust de besluitvorming omtrent inrichting van toegang tot basisregistraties, zoals de basisregistratie personen en de basisregistratie voertuigen, binnen de bevoegdheden van de Partijen bij het SupBRS. Met NatuurNetwerk is door alle Partijen een Verwerkersovereenkomst gesloten (zie annex 2 bij dit Convenant).

2.2. Verantwoordelijkheid verwerking van Politiegegevens door Boa's en het inzien van Politiegegevens door andere Boa's.

Partijen hebben ieder een licentie voor het gebruik van het BRS en autoriseren de bij hen in dienst zijnde of ten behoeve van hen werkzame Boa's om Politiegegevens in het BRS te verwerken. De autorisatie is afhankelijk van de wettelijke opsporingsbevoegdheid van de Boa en wordt begrensd door de wettelijke opsporingsbevoegdheid zoals vermeld in de akte van opsporingsbevoegdheid. Partijen zijn ieder Verwerkingsverantwoordelijke voor de eigen gegevensverwerkingen in de afzonderlijke compartimenten van het BRS door de Boa's die bij hen in dienst zijn of ten behoeve van hen werkzaam zijn. Voorts zijn Partijen ieder afzonderlijk Verwerkingsverantwoordelijke voor de verdere verwerking van Politiegegevens die de Boa's die bij hen in dienst zijn of ten behoeve van hen werkzaam zijn

verkrijgen, al dan niet van een andere Boa door gebruikmaking van het BRS.

Toelichting: Er wordt onderscheid gemaakt tussen de gezamenlijke inrichting van het BRS als systeem door de Verwerkingsverantwoordelijken in het SupBRS en de afzonderlijke verantwoordelijkheid voor de onderliggende verwerkingen in dat deel van het BRS waar de Boa's gegevens in verwerken. Het SupBRS draagt er zorg voor dat binnen het systeem niet meer Politiegegevens kunnen worden uitgewisseld dan nodig is voor de opsporingstaak van de Boa's. De gezamenlijke verantwoordelijkheid ziet aldus op de inrichting van het systeem voor verwerking van Politiegegevens, maar niet op de (details van de) gegevensverwerking door de Boa in de opsporingsfase en niet op de rapportage. (Samenwerkingsverbanden van) Werkgevers die als licentiehouder van het BRS gebruik maken, zijn zelf Verwerkingsverantwoordelijke voor gegevensverwerking in het eigen 'compartiment'. Onder verantwoordelijkheid van zijn werkgever of een samenwerkingsverband van werkgevers bepaalt de Boa of het noodzakelijk is bepaalde gegevens(verwerkingen) in het BRS uit te wisselen met of te raadplegen van andere Boa's. In het BRS is onder gezamenlijke verantwoordelijkheid van het SupBRS een systeem voor autorisaties voor toegang tot Politiegegevens gecreëerd. De autorisaties worden ingericht op basis van de akte van opsporingsbevoegdheid van de Boa, meer specifiek het domein en de wettelijke bevoegdheid van de Boa. De Boa beslist daar niet zelf over.

3. Rechtmatige verwerking van Politiegegevens in het BRS: welke gegevens mag de Boa in het BRS verwerken?

3.1 Partijen verplichten zich ertoe en zullen de Boa's instrueren om op hen rustende verplichtingen op grond van wet- en regelgeving inzake de bescherming van Persoonsgegevens en Politiegegevens na te leven.

3.2 De Boa mag niet meer Politiegegevens verwerken dan noodzakelijk is voor een goede vervulling van zijn specifieke wettelijke taak. De noodzaak om Politiegegevens te verzamelen, registreren, raadplegen en verstrekken wordt ingevuld door de opsporingstaak van de Boa.

3.3 Partijen verplichten zich ertoe de Boa te instrueren:
- dat hij Politiegegevens in BRS alleen verwerkt indien en zolang dit noodzakelijk is voor het realiseren van de in artikel 4 genoemde doeleinden en hierbij niet meer Politiegegevens verwerkt dan voor het realiseren van deze doeleinden noodzakelijk is.
- dat hij de nodige maatregelen treft opdat Politiegegevens worden verwijderd of vernietigd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt of dit door enige wettelijke bepaling wordt vereist;
- dat hij Politiegegevens slechts verwerkt, voor zover deze gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn;
- dat hij zorg draagt voor vernietiging of rectificatie als blijkt dat Politiegegevens gelet op de doeleinden waarvoor deze worden verwerkt, onjuist zijn;
- dat hij, voor zover praktisch uitvoerbaar, de kwaliteit van Politiegegevens controleert, voordat de gegevens worden verstrekt;

- dat hij bij de verstrekking van Politiegegevens de noodzakelijke informatie toevoegt aan de hand waarvan de ontvanger de mate van juistheid, volledigheid, betrouwbaarheid en actualiteit van Politiegegevens kan beoordelen;
- dat, voor zover mogelijk, Politiegegevens die op feiten zijn gebaseerd onderscheiden worden van Politiegegevens die op een persoonlijk oordeel zijn gebaseerd;
- dat hij onderscheid maakt tussen verschillende categorieën van Betrokkenen;
- dat hij Politiegegevens ter beschikking stelt aan de officier van justitie, voor zover deze de gegevens behoeft in verband met zijn gezag of zeggenschap over de Boa;
- dat hij Politiegegevens overeenkomstig artikel 15 Wpg deelt met ieder die geautoriseerd is voor de verwerking van Politiegegevens, voor zover diegene deze gegevens nodig heeft voor de uitvoering van zijn taak;
- dat hij Politiegegevens geheim houdt, tenzij de Verwerkingsverantwoordelijke hem opdraagt Politiegegevens te verstrekken aan derden, overeenkomstig het Besluit en de Wpg..

Toelichting: Deze norm wordt voor de Boa's nader ingevuld door het Besluit buitengewoon opsporingsambtenaar (verder: BBO) en de Circulaire Buitengewoon Opsporingsambtenaar (verder: Circulaire) die de opsporingsbevoegdheden van Boa's regelen. Ten behoeve van de strafrechtelijke handhaving beschikken Boa's per domein over opsporingsbevoegdheden. De domeinen bevatten de maximale opsporingsbevoegdheden. Uitgangspunt van de Circulaire is dat de opsporingsbevoegdheid van de Boa zich dient te beperken tot hetgeen noodzakelijk is voor een goede uitoefening van de betreffende functie en het daaraan gekoppelde takenpakket. De Boa-werkgever of het samenwerkingsverband van Boa-werkgevers dient het pakket aan opsporingsbevoegdheden te koppelen aan de taakomschrijving van de Boa die ten behoeve van hem werkzaam is. De Minister van Justitie en Veiligheid verleent een akte van opsporingsbevoegdheid. De opsporingsbevoegdheden van de Boa zoals genoemd in de akte gelden voor heel Nederland. Het werkgebied van de Boa is het gebied waarop de desbetreffende persoon zijn functie uitoefent in verband waarmee hij tot Boa wordt beëdigd (artikel 19 BBO) en wordt bepaald door zijn werkgever of het samenwerkingsverband van werkgevers ten behoeve waarvan hij werkzaamheden verricht.

4. Doelen en doelbinding

4.1 Partijen zullen er zorg voor dragen dat in het BRS slechts Politiegegevens worden verwerkt, voor zover dit noodzakelijk is voor de volgende doeleinden:

a) het houden van toezicht op naleving en handhaving van wetgeving door de Boa's binnen het kader van hun wettelijke opsporingstaken;
b) het opsporen van strafbare feiten door de Boa's binnen het kader van hun wettelijke opsporingstaken;
c) het verrichten van een concreet opsporingsonderzoek op verzoek van een officier van justitie;
d) het samenwerken met andere bevoegde opsporingsinstanties binnen het kader van hun wettelijke taken;
e) het samenstellen en op verzoek beschikbaar stellen van anonieme rapportages op basis van in BRS verwerkte gegevens;
f) het verstrekken van Politiegegevens conform de Verstrekkingenwijzer Wpg voor Boa's,

vastgesteld overeenkomstig het Besluit en de Wpg en gepubliceerd in BRS, alsmede;

i) het informeren van de (direct)toezichthouders, (het samenwerkingsverband van) de werkgever en de desbetreffende Boa indien er sprake is van een klacht gericht tegen het optreden van een Boa;

ii) het verstrekken van gegevens uit BRS ten behoeve van beleidsinformatie, wetenschappelijk onderzoek en statistiek aan daartoe gekwalificeerde onderzoekers of onderzoeksinstituten.

4.2 Partijen zullen er zorg voor dragen dat in het BRS slechts Persoonsgegevens van contactpersonen van Verwerkingsverantwoordelijken en Persoonsgegevens van Boa's worden verwerkt, voor zover dit gegeven de in artikel 4.1 onder a tot en met e genoemde doeleinden van verwerken van Politiegegevens noodzakelijk is, en dat slechts Persoonsgegevens van Boa's worden verwerkt voor zover dit noodzakelijk is voor het functioneren van technische voorzieningen, waaronder communicatievoorzieningen. In BRS kunnen Persoonsgegevens van Boa's worden verwerkt voor het faciliteren van communicatie tussen Boa's via beveiligde applicaties, en voor noodmeldingen alsmede voor operationele aansturing van Boa's.

5. Beveiliging, autorisaties, rechtstreekse toegang en logging

5.1 Partijen zijn verplicht om passende technische en organisatorische maatregelen te treffen om Politiegegevens in BRS te beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging. Zij dragen er gezamenlijk in het SupBRS zorg voor dat deze maatregelen, rekening houdend met de stand van de techniek, de kosten van de tenuitvoerlegging, en rekening houdend met de aard, de reikwijdte, de context en de doeleinden van de verwerking, alsmede met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen een passend beveiligingsniveau garanderen.

5.2 Partijen onderhouden een systeem van autorisaties voor verwerking van Politiegegevens in BRS en verstrekking van Politiegegevens in BRS dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Politiegegevens in BRS worden slechts verwerkt door personen die daartoe zijn geautoriseerd en voor zover de autorisatie strekt.

5.3 Partijen autoriseren de Boa's die bij hen in dienst zijn of ten behoeve van hen werkzaam zijn voor de verwerking van Politiegegevens in BRS ter uitvoering van de onderdelen van de opsporingstaak waarmee zij zijn belast. De autorisatie bevat een duidelijke omschrijving van de verwerkingen waartoe de betreffende Boa wordt geautoriseerd en de onderdelen van de wettelijke opsporingstaak ter uitvoering waarvan de verwerkingen worden gedaan.

5.4 Partijen kunnen ieder voor zich overeenkomstig artikel 3 van het Besluit voor specifieke

vormen van verwerking van Politiegegevens in BRS een beroep doen op een persoon die onder hun beheer valt en die geen Boa is. In de autorisatie worden vastgelegd het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort Politiegegevens en de categorieën van Betrokkenen. Partijen zullen daartoe gebruik maken van de modelverklaring voor autorisatie gepubliceerd in BRS.

5.5 Partijen instrueren de Boa's die voor of ten behoeve van hen werkzaam zijn alsmede personen die overeenkomstig artikel 5.4 geautoriseerd zijn om zich bij het verwerken van Politiegegevens in het BRS te houden aan de systeembeveiliging zoals bepaald door de Partijen in het SupBRS.

5.6 Partijen dragen zorg voor de vastlegging langs elektronische weg (logging) van ten minste de volgende verwerkingen van Politiegegevens in BRS: het verzamelen, wijzigen, raadplegen, verstrekken onder meer in de vorm van doorgiften, combineren of vernietigen van Politiegegevens. De aldus vastgelegde gegevens worden uitsluitend gebruikt voor de controle van de rechtmatigheid van de gegevensverwerking, voor interne controles, ter waarborging van de integriteit en de beveiliging van de Politiegegevens en voor strafrechtelijke procedures.

Toelichting: de uitvoering van de beveiliging, het systeem van autorisaties en logging van gebruik wordt aan de Verwerker NatuurNetwerk uitbesteed en is onderdeel van de Verwerkersovereenkomst (annex 2). Partijen dienen de Boa te instrueren dat de beveiligingsgegevens (multi-factor authenticatie) niet met anderen gedeeld mogen worden.

6. Bewaren en verwijderen van Politiegegevens

6.1 Politiegegevens worden in het BRS niet langer bewaard dan noodzakelijk is voor het realiseren van de in artikel 4 genoemde doelen, conform de Bewaartermijnenwijzer Wpg voor Boa's, vastgesteld overeenkomstig de Wpg en gepubliceerd in BRS.

6.2 Indien Partijen hard-copy of op andere wijze buiten BRS Politiegegevens verwerken die via BRS verkregen zijn, dragen Partijen zelf zorg voor verwijdering en vernietiging van deze gegevens, conform hetgeen is bepaald in artikel 6.1.

6.3 Indien Partijen overgaan tot verdere verwerking van Politiegegevens in BRS in het kader van de uitvoering van de politietaak zullen zij conform artikel 13 Wpg en de Bewaartermijnenwijzer Wpg voor Boa's, in BRS de volgende kenmerken vastleggen: het doel waarvoor de Politiegegevens verder worden verwerkt, de categorieën van Betrokkenen over wie gegevens verder verwerkt worden, de soorten over hen op te nemen gegevens en de gevallen waarin of termijnen waarbinnen de verwerking wordt beëindigd.

7. Verwerker

Partijen geven gezamenlijk opdracht aan NatuurNetwerk als Verwerker om het technisch en functioneel beheer van BRS in te richten en te onderhouden en de daarin opgenomen Politiegegevens te verwerken en te bewaren conform de gezamenlijke instructies van Partijen in het SupBRS.

Het SupBRS draagt er zorg voor dat NatuurNetwerk de Politiegegevens slechts verwerkt in opdracht van de Verwerkingsverantwoordelijken, geheimhouding betracht en passende technische en organisatorische beveiligingsmaatregelen treft met betrekking tot de te verrichten verwerkingen.

De afspraken tussen de Partijen en NatuurNetwerk zijn vastgelegd in een Verwerkersovereenkomst (annex 2 bij het Convenant).

Toelichting: Verwerkingsverantwoordelijken sluiten ieder bijgaande verwerkersovereenkomst met NatuurNetwerk voor de gegevensverwerking in het BRS.

RECHTEN VAN BETROKKENEN

8 Digitaal aanspreekpunt

8.1. Een Betrokkene kan zich naar aanleiding van optreden door een Boa, rechtstreeks wenden tot die Boa, maar ook tot (het samenwerkingsverband van) de werkgever van de Boa. Verzoeken, vragen en klachten die betrekking hebben op verwerking van Politiegegevens door een Boa zal (het samenwerkingsverband van) de werkgever in behandeling nemen. De Betrokkene kan ook terecht op de website www.privacyvragenbrs.nl. Deze website is ingericht conform de instructies van Partijen in het SupBRS en doet dienst als digitaal aanspreekpunt en klachtenloket voor Betrokkenen in verband met de verwerking van Politiegegevens in het BRS.

8.2 De website www.privacyvragenbrs.nl. biedt:

a) publieksvoorlichting over het BRS.
b) publieksvoorlichting over de doeleinden en de werking van het BRS, de verdeling van verantwoordelijkheid voor de gegevensverwerking in het BRS en de wijze waarop de Betrokkenen hun rechten kunnen uitoefenen.
c) de mogelijkheid voor Betrokkenen om verzoeken om inzage in, rectificatie, vernietiging of afscherming van Politiegegevens in BRS te sturen aan het digitaal aanspreekpunt. Het digitaal aanspreekpunt zal de verzoeken die betrekking hebben op de verwerking van Politiegegevens in het BRS doorsluizen naar de Verwerkingsverantwoordelijke die het betreft.

Toelichting: bij het Convenant zijn diverse Partijen betrokken. Ten einde te voorkomen dat de Betrokkene niet weet bij wie hij zich moet melden en om te voorkomen dat de verantwoordelijkheid voor de uitvoering van het Convenant en de inrichting en uitvoering van het BRS te veel versnippert, vervult het Ministerie van Justitie en Veiligheid de regierol voor het SupBRS. Voor Betrokkenen is er een website ingericht als digitaal aanspreekpunt voor klachten, vragen en opmerkingen met betrekking tot de verwerking van Politiegegevens in het BRS. Het SupBRS geeft aan de Verwerker NatuurNetwerk de opdracht om vragen, opmerkingen en klachten naar de juiste Verwerkingsverantwoordelijke door te sturen. Daarnaast kunnen Betrokkenen ook rechtstreeks bij de Boa's en (samenwerkingsverbanden van) Boa-werkgevers terecht met vragen, opmerkingen en klachten. Het digitaal loket is bedoeld als extra aanspreekpunt, zodat de Betrokkene altijd een makkelijke route heeft om zijn vragen, opmerkingen en klachten bij de juiste Verwerkingsverantwoordelijke voor de verwerking van zijn Politiegegevens te deponeren.

9. Instructie van de Boa over rechten van Betrokkenen

Partijen instrueren de voor of ten behoeve van hen werkzame Boa's om Betrokkenen te informeren over hun recht op informatie over de verwerking van Politiegegevens in BRS, en hun recht op inzage in, rectificatie, vernietiging of afscherming van Politiegegevens in het BRS in lijn met hetgeen is opgenomen in de bepalingen 10, 11 en 12.

10. Recht op informatie over de verwerking van Politiegegevens in BRS

10.1 Partijen verstrekken aan Betrokkenen in elk geval de volgende informatie over de verwerking van Politiegegevens in BRS in de vorm van een privacystatement voor BRS:
a. de identiteit en contactgegevens van de Verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;
b. de verwerkingsdoelen van de Politiegegevens, genoemd in bepaling 4;
c. de rechten van de Betrokkene, bedoeld in de bepalingen 11 en 12 en het recht een klacht in te dienen bij de Autoriteit persoonsgegevens, en de contactgegevens van die autoriteit;
d. de rechtsgrondslag van de verwerking;
e. de bewaartermijn van de Politiegegevens;
f. in voorkomend geval, de categorieën van de ontvangers van de Politiegegevens.

10.2 De tekst van het privacystatement voor BRS wordt door Partijen gezamenlijk vastgesteld en wordt door Partijen beschikbaar gesteld via de eigen websites van Partijen en/of er wordt doorgelinkt naar de website www.privacyvragenbrs.nl.

Toelichting: op grond van de Wpg moeten de werkgevers van de Boa's als Verwerkingsverantwoordelijken of het samenwerkingsverband dat zij als Gemeenschappelijke Verwerkingsverantwoordelijke hebben aangewezen invulling geven aan alle wettelijke verplichtingen, waaronder de informatieplicht. In het SupBRS zal het standaard privacystatement worden vastgesteld dat Partijen kunnen gebruiken om invulling te geven aan de informatieplicht. Dit privacystatement kan

de Betrokkene vinden op de website www.privacywragenbrs.nl en via de eigen privacystatements op de website van Partijen. Partijen kunnen in het eigen privacystatement linken naar het Privacystatement BRS.

11. Recht op inzage Politiegegevens in BRS

11.1 Partijen zullen aan Betrokkene op diens schriftelijke verzoek binnen zes weken uitsluitsel geven over de verwerking van hem betreffende Politiegegevens in BRS en, wanneer dat het geval is, inzage geven in die Politiegegevens en informatie verstrekken over:
a. de doelen en de rechtsgrond van de verwerking;
b. de betrokken categorieën van Politiegegevens;
c. of deze Betrokkene betreffende Politiegegevens gedurende een periode van vier jaar voorafgaande aan het verzoek zijn verstrekt en zo ja, informatie geven over de (categorieën van) ontvangers aan wie de gegevens zijn verstrekt;
d. de bewaartermijn van de Politiegegevens of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
e. het recht van Betrokkene te verzoeken om rectificatie, vernietiging of afscherming van de verwerking van hem betreffende Politiegegevens;
f. het recht een klacht in te dienen bij de Autoriteit persoonsgegevens, en de contactgegevens van de autoriteit;
g. de herkomst, voor zover beschikbaar, van hem betreffende Politiegegevens.

11.2 De Verwerkingsverantwoordelijke kan zijn beslissing voor ten hoogste vier weken verdagen. Van de verdaging wordt schriftelijk mededeling gedaan.

Toelichting: op grond van de Wpg moet de werkgever van de Boa als Verwerkingsverantwoordelijke, of het samenwerkingsverband dat zij als Gemeenschappelijke Verwerkingsverantwoordelijke hebben aangewezen, invulling geven aan alle wettelijke verplichtingen, waaronder het recht op inzage van Politiegegevens in BRS. In het SupBRS zal de procedure voor het uitoefenen van rechten van Betrokkenen worden vastgesteld. Verzoeken kunnen worden ingediend via het digitaal aanspreekpunt. Conform de procedure voor het uitoefenen van rechten van Betrokkenen via het digitaal aanspreekpunt draagt Verwerker NatuurNetwerk zorg voor het volgende: vaststelling van de identiteit van de Betrokkene; verzending van een ontvangstbevestiging en doorgeleiding van het verzoek naar de Verwerkingsverantwoordelijke die het betreft.

12. Recht op rectificatie en vernietiging van Politiegegevens in BRS

12.1 Partijen zullen op schriftelijk verzoek van de Betrokkene hem betreffende onjuiste Politiegegevens in BRS rectificeren en, rekening houdend met het doel van de verwerking, onvolledige Politiegegevens aanvullen, onder meer door middel van een aanvullende verklaring. Het verzoek van Betrokkene dient de aan te brengen wijzigingen te bevatten.

12.2 Op schriftelijk verzoek van de Betrokkene vernietigen Partijen hem betreffende Politiegegevens in BRS indien de gegevens in strijd met een wettelijk voorschrift worden verwerkt of om te voldoen aan een wettelijke verplichting.

12.3 In plaats van vernietiging dragen Partijen zorg voor afscherming als:
a. de juistheid van de gegevens door de Betrokkene wordt betwist en de juistheid of onjuistheid niet kan worden geverifieerd; of
b. de gegevens moeten worden bewaard als bewijsmateriaal.

12.4 Partijen stellen de Betrokkene binnen vier weken schriftelijk in kennis met betrekking tot de opvolging van zijn verzoek.

12.5 Partijen geven de rectificatie van de onjuiste Politiegegevens door aan de bevoegde autoriteit van wie de gegevens afkomstig zijn.

12.6 Indien Partijen Politiegegevens hebben gerectificeerd, vernietigd of afgeschermd, stellen zij de ontvangers daarvan in kennis.

Toelichting: op grond van de Wpg moet de werkgever van de Boa als Verwerkingsverantwoordelijke of het samenwerkingsverband van werkgevers als aangewezen gemeenschappelijke verwerkingsverantwoordelijke invulling geven aan alle wettelijke verplichtingen, waaronder het recht op rectificatie en vernietiging van Politiegegevens in BRS. In het SupBRS zal de procedure voor het uitoefenen van rechten van Betrokkenen worden vastgesteld. Verzoeken kunnen worden ingediend via het digitaal aanspreekpunt. Conform de procedure voor het uitoefenen van rechten van Betrokkenen via het digitaal aanspreekpunt draagt Verwerker NatuurNetwerk zorg voor het volgende: vaststelling van de identiteit van de Betrokkene; verzending van een ontvangstbevestiging en doorgeleiding van het verzoek naar de Verwerkingsverantwoordelijke die het betreft.

13. Uitzonderingen op rechten van Betrokkenen

13.1 Partijen kunnen weigeren aan een verzoek om inzage dan wel rectificatie of vernietiging van Politiegegevens in BRS gehoor te geven voor zover dit noodzakelijke en evenredig is:
a. ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures;
b. ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen;
c. ter bescherming van de openbare veiligheid;
d. ter bescherming van de rechten en vrijheden van derden;
e. ter bescherming van de nationale veiligheid;
f. ingeval van een kennelijk ongegrond of buitensporig verzoek.

13.2 Een gehele of gedeeltelijke afwijzing van een verzoek als bedoeld in het eerste lid is schriftelijk en bevat de redenen voor de afwijzing.

OVERIGE BEPALINGEN

14 Regie met betrekking tot de uitvoering van het Convenant

Het Ministerie van Justitie en Veiligheid vervult de regierol ten aanzien van de uitvoering van dit Convenant.

De regierol omvat in ieder geval:

a) Organiseren van overleg met de betrokken Partijen teneinde verzoeken tot wijziging van het Convenant met de Regiegroep te bespreken;

b) Organiseren van een jaarlijks overleg teneinde de werking en uitvoering van het Convenant te evalueren en daarvan verslag te doen;

Toelichting: In praktijk zal een toekomstige Partij bij het Convenant een licentie voor BRS van NatuurNetwerk afnemen en zal de aanmelding bij het SupBRS door NatuurNetwerk als Verwerker worden gefaciliteerd. Voor verzoeken tot wijziging van het Convenant wordt een contactpunt op de website www.boaregistratie.nl ingericht (emailadres: info@boaregistratie.nl).

15 Nieuwe toetreding, wijzigingen en aanvullingen van het Convenant en besluitvorming

15.1 Alleen organisaties en instanties die een licentie hebben voor het gebruik van het BRS en ten behoeve waarvan Boa's werkzaamheden verrichten, treden toe tot het SupBRS.

15.2 Toetreding tot het SupBRS vindt plaats door ondertekening van dit Convenant. Een organisatie of instantie wordt daardoor "Partij" bij het Convenant.

15.3 Elke Partij wijst een contactpersoon aan ten behoeve van overleggen, besluitvorming, coördinatie en overige communicatie met betrekking tot het SupBRS en is ingedeeld bij een TGG.

15.4 Elke TGG kan bij de Regiegroep een verzoek indienen tot wijziging van het Convenant. De Regiegroep zal het Ministerie van Justitie en Veiligheid verzoeken om een overleg te organiseren teneinde de gevraagde wijziging te bespreken.

15.5 Ieder van de Partijen verleent aan de Regiegroep een onherroepelijke bijzondere volmacht in de zin van artikel 3:62 lid 2 van het Burgerlijk Wetboek ('BW') om namens hen in te stemmen met wijzigingen van het Convenant en de Annexes daarbij (inclusief de Verwerkersovereenkomst met NatuurNetwerk). Besluiten tot wijziging van het Convenant worden door de Regiegroep genomen conform het Reglement Regiegroep De gewijzigde versie van het Convenant wordt onverwijld aan alle Partijen verstrekt.

15.6 Partijen waarborgen dat zij de contactpersonen bij hun TGG, tijdig en adequaat op de hoogte houden van relevante gebeurtenissen die kunnen leiden tot wijzigingen in de beoogde samenwerking van SupBRS.

15.7 Met betrekking tot wijzigingen in het BRS geldt het volgende:

- Boa's kunnen verzoeken doen tot wijziging van de software die de operationele gegevensverwerking betreffen, maar geen significante invloed hebben op de werkprocessen of inrichting van het systeem dan wel de gegevensuitwisseling binnen het systeem (Categorie I vragen);
- Indien verzoeken significante invloed hebben op werkprocessen kan de werkgever die, of het samenwerkingsverband van werkgevers dat Partij is bij dit Convenant een verzoek indienen bij zijn TGG (Categorie II vragen). Een TGG besluit of uitvoering van een categorie II vraag wenselijk en nodig is en geeft daartoe namens de werkgevers binnen een TGG instructies aan de Verwerker NatuurNetwerk;
- Het SupBRS bepaalt in geval van verzoeken tot wijzigingen inzake de inrichting van het systeem voor verwerking/uitwisseling van Politiegegevens of systeemwijziging wenselijk en nodig is en geeft daartoe instructies aan de Verwerker NatuurNetwerk (Categorie III vragen). Partijen machtigen de Regiegroep om besluiten te nemen naar aanleiding van Categorie III vragen en om daarmee verband houdende instructies te geven aan de Verwerker NatuurNetwerk.

158 Partijen machtigen de Regiegroep om de volgende bevoegdheden uit te oefenen: anonieme rapportages opstellen op basis van de gegevensverwerking in BRS; besluiten nemen naar aanleiding van een verzoek om beschikbaarstelling van deze rapportages; daarmee verband houdende instructies geven aan de Verwerker NatuurNetwerk.

15.9 Partijen machtigen de Regiegroep om besluiten te nemen naar aanleiding van een verzoek van daartoe gekwalificeerde onderzoekers of onderzoeksinstituten tot verstrekking van gegevens uit het BRS ten behoeve van onderzoek voor wetenschappelijke of statistische doeleinden en om daarmee verband houdende instructies te geven aan de Verwerker NatuurNetwerk.

15.10 Het Ministerie van Justitie en Veiligheid organiseert minimaal 1 maal per jaar, of zo vaak als wenselijk of nodig is, overleg met de Regiegroep over het SupBRS.

15.11 Voor een overleg van de Regiegroep worden alle vertegenwoordigers van TGG's die zitting hebben in de Regiegroep uitgenodigd. Eventuele stemming over wijziging van het Convenant vindt plaats tijdens overleg van de Regiegroep.

De Verwerker NatuurNetwerk zal in opdracht van het SupBRS uitvoering geven aan de verzoeken tot wijziging en overige opdrachten tot gegevensverwerking.

Annex 1 bij Convenant SupBRS 2020

PARTIJEN

In BRS wordt real time een lijst bijgehouden van alle Partijen en de TGG waarin zij zijn ingedeeld. De real time lijst is beschikbaar voor contactpersonen van werkgevers of van samenwerkingsverbanden van werkgevers binnen een TGG en omvat de volgende informatie:

- in welke TGG de werkgever of het samenwerkingsverband is ingedeeld,
- wie in de TGG zitten,
- het reglement van de TGG's,
- een mogelijkheid om contact op te nemen met de TGG,
- wie de TGG vertegenwoordigt in de Regiegroep,
- het reglement van de Regiegroep.

De toezichthouder en direct toezichthouder van de Boa's kunnen op verzoek toegang krijgen tot BRS.

Voor akkoord namens de Partijen:

Naam Partij: [redacted]
Staatsbosbeheer

Handtekening.....
namens Verwerkingsverantwoordelijke

Naam ondertekenaar:
DMJ Kamphuis

Contactpersoon SupBRS: [redacted]

Opgemaakt te:
Amersfoort

De dato:
21-9-20

Paraaf licentiehouder [redacted]

16. Looptijd van het Convenant

Dit Convenant wordt aangegaan voor onbepaalde tijd.

17. Opzegging

17.1 Elke Partij kan het Convenant schriftelijk opzeggen met inachtneming van een termijn van 2 maanden. Door opzegging van het Convenant eindigt de deelname aan het SupBRS. Opzegging van het Convenant leidt tevens tot beëindiging van toegang tot BRS en tot beëindiging van de licentieovereenkomst met NatuurNetwerk zoals bepaald in de licentieovereenkomst met NatuurNetwerk.

17.2 Beëindiging van de licentieovereenkomst met NatuurNetwerk leidt tot opzegging van dit Convenant en daarmee tot beëindiging van de deelname aan het SupBRS.

17.3 Wanneer een Partij dit Convenant opzegt, blijft het Convenant voor de overige Partijen in stand, voor zover de inhoud en de strekking daarvan zich daartegen niet verzetten.

18. Evaluatie

Partijen zullen de uitvoering en werking van dit Convenant jaarlijks evalueren. De Regiegroep organiseert in overleg met het Ministerie van Justitie en Veiligheid daartoe jaarlijks een overleg waarvoor de Regiegroep leden als vertegenwoordigers van Partijen worden uitgenodigd. Partijen kunnen bij de contactpersonen van hun TGG input leveren voor de evaluatie. De notulen van de evaluatie worden door de Regiegroep leden aan Partijen in hun achterban toegestuurd of beschikbaar gesteld via www.boaregistratie.nl.

SLOTBEPALINGEN

19. Inwerkingtreding

Dit Convenant treedt in werking met ingang van de datum waarop de Wet politiegegevens van toepassing is op de gegevensverwerking door Boa's.

20. Citeertitel

Dit Convenant wordt aangehaald als: Convenant SupBRS 2020.

Toelichting grondslagen

In dit document kunt u secties vinden die onleesbaar zijn gemaakt. Deze informatie is achterwege gelaten op basis van de Wet open overheid (Woo). De letter die hierbij is vermeld correspondeert met de bijbehorende grondslag in onderstaand overzicht.

J Art. 5.1 lid 2 sub e

Het belang van de openbaarmaking van deze informatie weegt niet op tegen het belang van de eerbiediging van de persoonlijke levenssfeer van betrokkenen

Annex 2 bij Samenwerkingsverband uitwisseling Politiegegevens BRS

VERWERKERSOVEREENKOMST

TUSSEN:
Een partij die deelneemt aan het Samenwerkingsverband uitwisseling politiegegevens BRS en een licentie heeft op het Boa Registratie Systeem (hierna: "**Verwerkingsverantwoordelijke**")

EN

NatuurNetwerk B.V., een besloten vennootschap naar Nederlands recht, statutair gevestigd te Vaassen op de Hofsemolenweg 8 en kantoorhoudende te Vaassen op de Hofsemolenweg 8, zoals geregistreerd bij de Kamer van Koophandel onder nummer 08155147 (hierna "**Verwerker**" of "NatuurNetwerk").

SAMEN AAN TE DUIDEN ALS "PARTIJEN"

KOMEN HIERBIJ OVEREEN:

1. Onderwerp van deze Verwerkersovereenkomst

1.1. Deze Verwerkersovereenkomst is alleen van toepassing op de verwerking van Politiegegevens en Persoonsgegevens in het kader van het convenant Samenwerkingsverband uitwisseling politiegegevens BRS (hierna aan te duiden als het "Convenant" en het "SupBRS") dat is gesloten tussen partijen die een licentieovereenkomst hebben gesloten met NatuurNetwerk (hierna aan te duiden als "Licentieovereenkomst") voor het gebruik van het Boa Registratie Systeem (hierna aan te duiden als "BRS").

1.2. Begrippen als "Verwerking", "Persoonsgegevens", "Politiegegevens", "Verwerkingsverantwoordelijke", "Verwerker", "Technische Gebruikers Groep" of "TGG" en "Regiegroep" hebben de betekenis die daaraan is gegeven in het Convenant.

1.3. In het kader van de uitvoering van het Convenant kunnen Verwerkingsverantwoordelijken

a) gezamenlijk aan Verwerker opdrachten geven ten aanzien van:

- de inrichting van het systeem voor verwerking van Politiegegevens in het BRS met inbegrip van beveiligde applicaties voor communicatie tussen Boa's;

Paraaf licentiehouder J NatuurNetwerk J

- de wijze waarop Politiegegevens binnen het BRS kunnen worden uitgewisseld tussen de Boa's die in dienst zijn van of werkzaam zijn voor Partijen die de Licentieovereenkomst hebben gesloten;

- de wijze waarop Politiegegevens in het BRS toegankelijk kunnen zijn voor (samenwerkingsverbanden van) werkgevers, politie, justitie en overige opsporingsdiensten;

- de wijze waarop Politiegegevens in het BRS kunnen worden verstrekt aan derde partijen;

- de wijze waarop gegevens in het BRS kunnen worden verstrekt voor beleidsinformatie, wetenschappelijk onderzoek en statistiek;

- de wijze waarop door een Boa zelf verzamelde Politiegegevens in het BRS kunnen worden onderscheiden van andere Politiegegevens;

b) ieder voor zich opdrachten geven ten aanzien van de verwerking van Politiegegevens door de Boa's in het eigen compartiment in het BRS.

2. Verwerkingsverantwoordelijke en Verwerker

2.1. Verwerker zal optreden als Verwerker en Verwerkingsverantwoordelijke als Verwerkingsverantwoordelijke.

2.2. Verwerker zal Politiegegevens en Persoonsgegevens uitsluitend verwerken op een wijze die – en voor zover dit – noodzakelijk is voor de uitvoering van het Convenant of voor de uitvoering van de Licentieovereenkomst, behalve wanneer dit noodzakelijk is om te voldoen aan een op Verwerker rustende wettelijke verplichting of voor het opvolgen van instructies van Verwerkingsverantwoordelijke. In geen geval verwerkt Verwerker de Politiegegevens en Persoonsgegevens voor eigen doeleinden.

2.3. In het bijzonder kan Verwerkingsverantwoordelijke via zijn TGG of via de Regiegroep instructies geven ten aanzien van de inrichting van het BRS op het punt van autorisaties voor toegang en uitwisseling van Politiegegevens in BRS.

2.4. De Partijen verenigd in het SupBRS sluiten de Licentieovereenkomst af om te profiteren van de expertise van Verwerker als het gaat om het opslaan, uitwisselen en beveiligen van Politiegegevens voor de doeleinden uiteengezet in Annex 1. Het is Verwerker toegestaan om de middelen aan te wenden die hij noodzakelijk acht om die doeleinden na te streven.

2.5.

3. Vertrouwelijkheid

3.1. Verwerker zal alle Politiegegevens en Persoonsgegevens die worden verwerkt in het kader van de uitvoering van het Convenant en de Licentieovereenkomst als strikt vertrouwelijk behandelen en zal al haar werknemers, vertegenwoordigers en/of goedgekeurde sub-Verwerkers die betrokken zijn bij de verwerking van de vertrouwelijke aard van de gegevens op de hoogte stellen. Verwerker zal waarborgen dat dergelijke personen en partijen een adequate geheimhoudingsovereenkomst hebben getekend.

4. Beveiliging

4.1. Verwerker zal passende technische en organisatorische maatregelen nemen ter beveiliging van de verwerking van Politiegegevens en Persoonsgegevens, in ieder geval:

(a) maatregelen om te waarborgen dat Boa's slechts geautoriseerd zijn voor toegang tot het BRS in overeenstemming met hun wettelijke opsporingsbevoegdheden en dat niet-Boa's slechts geautoriseerd zijn voor toegang tot het BRS overeenkomstig de verklaring voor autorisatie van een niet Boa;

(b) maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Politiegegevens en Persoonsgegevens voor de doeleinden die uiteen zijn gezet in Annex 1;

(c) maatregelen om de Politiegegevens en Persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging.;

(d) maatregelen om de vastlegging langs elektronische weg (logging) te waarborgen van ten minste de volgende verwerkingen van Politiegegevens in BRS: het verzamelen, wijzigen, raadplegen, verstrekken onder meer in de vorm van doorgiften, combineren of vernietigen van Politiegegevens.

4.2. Verwerker heeft te allen tijde een passend beveiligingsbeleid geïmplementeerd voor de verwerking van de Politiegegevens en Persoonsgegevens, waarin zij in ieder geval de in artikel 4.1 opgesomde maatregelen uiteenzet. Verwerker zal op verzoek van Verwerkingsverantwoordelijke:

(a) Verwerkingsverantwoordelijke inzage bieden in het beveiligingsbeleid;

(b) aantonen welke maatregelen zij heeft genomen op basis van dit artikel 4;

(c) haar beveiligingsbeleid aanpassen overeenkomstig nadere, schriftelijke instructies van

Verwerkingsverantwoordelijke waarbij de kosten daarvan voor rekening komen van Verwerkingsverantwoordelijke.

5. Verbeteringen van de beveiliging

5.1. Partijen erkennen dat beveiligingseisen voortdurend veranderen en dat een effectieve beveiliging frequente evaluaties en regelmatige verbetering van verouderde beveiligingsmaatregelen vereist. Verwerker zal daarom de maatregelen zoals geïmplementeerd op grond van artikel 4 voortdurend evalueren en verscherpen, aanvullen of verbeteren om te blijven voldoen aan de eisen van artikel 4.

5.2. Verwerkingsverantwoordelijke heeft het recht om Verwerker te instrueren om aanvullende beveiligingsmaatregelen te nemen. Indien een wijziging van de Licentieovereenkomst vereist is om een dergelijke instructie op te volgen zullen Partijen te goeder trouw een wijziging van de Licentieovereenkomst overeenkomen. De kosten voor uitvoering van aanvullende beveiligingsmaatregelen komen voor rekening van Verwerkingsverantwoordelijke.

6. Rechten van Betrokkenen

6.1. Verwerker zal Verwerkingsverantwoordelijke met passende middelen bijstaan om naleving van de bepalingen in het Convenant betreffende de rechten van Betrokkenen te verzekeren. Verwerker beheert een website als digitaal aanspreekpunt voor klachten, vragen en opmerkingen van Betrokkenen met betrekking tot de Verwerking van Politiegegevens in het BRS en zal vragen, opmerkingen en klachten naar de juiste Verwerkingsverantwoordelijke doorsturen.

7. Gegevensverkeer

7.1 Verwerker zal Politiegegevens en Persoonsgegevens slechts (laten) verwerken in of doorvoeren, naar een land buiten de Europese Economische Ruimte zonder een passend beschermingsniveau, na instructie van de Verwerkingsverantwoordelijke.

8. Informatieplichten en incidentenmanagement

8.1 Verwerker stelt Verwerkingsverantwoordelijke onverwijld op de hoogte van incidenten met betrekking tot de verwerking van de Politiegegevens en Persoonsgegevens, zal Verwerkingsverantwoordelijke te allen tijde haar medewerking verlenen en zal de instructies van Verwerkingsverantwoordelijke ten aanzien van een dergelijk incident opvolgen, met als doel om Verwerkingsverantwoordelijke in staat te stellen een deugdelijk onderzoek te verrichten naar het

incident, een correcte respons te formuleren en passende vervolgstappen te nemen ten aanzien van het incident.

8.2 Onder "incident" zoals bedoeld in het vorige lid wordt in ieder geval het volgende verstaan:

(a) iedere ongeautoriseerde of onopzettelijke toegang, verwerking, verwijdering, verlies of enige vorm van onrechtmatige verwerking van de Politiegegevens en Persoonsgegevens;

(b) een doorbreking van de beveiliging en/of vertrouwelijkheid, zoals uiteengezet in artikel 3 en 4 van deze Verwerkersovereenkomst, die leidt tot onopzettelijke of onrechtmatige vernietiging, verlies, wijziging, onbevoegde openbaarmaking van – of toegang tot – de Politiegegevens of Persoonsgegevens, of enige aanwijzing dat een dergelijke inbreuk zal plaatsvinden of heeft plaatsgevonden.

8.3 Verwerker zal te allen tijde geschreven procedures voorhanden hebben die haar in staat stellen om Verwerkingsverantwoordelijke van een onmiddellijke reactie over een incident te voorzien, en om effectief samen te werken met Verwerkingsverantwoordelijke om het incident af te handelen, en zal Verwerkingsverantwoordelijke voorzien van een exemplaar van dergelijke procedures indien Verwerkingsverantwoordelijke daar schriftelijk om verzoekt.

9. Inschakelen van sub-Verwerkers

9.1 Verwerker zal haar activiteiten die (deels) bestaan uit het verwerken van de Politiegegevens of vereisen dat Politiegegevens verwerkt worden, en van Persoonsgegevens niet uitbesteden aan een derde partij zonder voorafgaande, schriftelijke toestemming van Verwerkingsverantwoordelijke.

9.2 Niet tegenstaande de toestemming van Verwerkingsverantwoordelijke, zoals bedoeld in het vorige lid, zal Verwerker volledig aansprakelijk blijven jegens Verwerkingsverantwoordelijke voor de gevolgen van het uitbesteden aan een derde in overeenstemming met artikel 11.

9.3 De Verwerker bewerkstelligt dat de sub-Verwerker gebonden is aan de verplichtingen die op de Verwerker rusten uit hoofde van deze Verwerkersovereenkomst en ziet toe op naleving daarvan.

10. Teruggave of vernietiging van de gegevens

10.1 Wanneer een einde komt aan het Convenant zal Verwerkingsverantwoordelijke Verwerker instrueren of en op welke wijze de verwerking en uitwisseling van Politiegegevens en Persoonsgegevens in BRS kan worden voortgezet dan wel de gegevens aan Verwerkingsverantwoordelijke moeten worden verstrekt of moeten worden gewist en kopieën

moeten worden verwijderd, tenzij opslag van de gegevens verplicht is. Eventuele kosten komen voor rekening van Verwerkingsverantwoordelijke.

10.2 Wanneer een Partij stopt met het gebruik van het BRS, dan zullen de in het BRS opgeslagen Politiegegevens en Persoonsgegevens door natuurlijk verloop van de bewaartermijnen worden verwijderd. Gedurende de bewaartermijn zullen de gegevens in BRS beschikbaar blijven voor de overige gebruikers van BRS, met inachtneming van hun wettelijke opsporingsbevoegdheden.

10.3 In overleg en met toestemming van de verantwoordelijke Officier van Justitie kunnen Politiegegevens die in BRS zijn opgeslagen door Boa's in dienst van of werkzaam voor een Partij ook beschikbaar worden gesteld aan die Partij wanneer hij stopt met het gebruik van BRS. Eventuele kosten voor dit beschikbaar stellen komen voor rekening van die Partij.

11. Aansprakelijkheid en vrijwaring

11.1 Verwerker is jegens Verwerkingsverantwoordelijke uitsluitend aansprakelijk voor schade die het directe gevolg is van niet nakoming van Verwerker van de instructies van Verwerkingsverantwoordelijke, voor zover die instructies uitdrukkelijk in deze Verwerkersovereenkomst zijn opgenomen. De aansprakelijkheid van Verwerker voor een incident of een reeks van samenhangende incidenten is beperkt tot het bedrag dat de aansprakelijkheidsverzekeraar in dat verband aan Verwerker uitkeert.

11.2 Zonder afbreuk te doen aan de aansprakelijkheid van Verwerkingsverantwoordelijke op grond van de wet, is Verwerkingsverantwoordelijke jegens Verwerker voorts aansprakelijk en stelt Verwerker schadeloos voor alle sancties, claims, acties, aanspraken van derden en voor verliezen, schade of kosten die aan de zijde van Verwerker vallen en die rechtstreeks of indirect voortvloeien uit of tot stand komen in verband met een tekortkoming van deze Verwerkersovereenkomst door Verwerkingsverantwoordelijke.

Handtekening [redacted] .....
namens Verwerkingsverantwoordelijke

Naam: DMJ Kamphuis

Namens: Staatsbosbeheer

Functie: dev. Directeur

Datum: 21-9-20

Handtekening [redacted] .....
namens Verwerker

Naam: [redacted]

Namens: NatuurNetwerk BV

Functie: Directeur

Datum: 25-06-2020

12. Informatie en audits

12.1. Op verzoek van de Verwerkingsverantwoordelijke zal de Verwerker alle informatie verstrekken die voor de Verwerkingsverantwoordelijke noodzakelijk is om nakoming van deze verwerkersovereenkomst aan te tonen.

12.2. Verwerker zal jaarlijks een beveiligingsaudit uitvoeren en Verwerkingsverantwoordelijke informeren over de uitkomst daarvan.

13. Duur en beëindiging

13.1 Elke Partij die een licentie heeft op het BRS sluit met Verwerker deze Verwerkersovereenkomst. Deze Verwerkersovereenkomst treedt in werking op de datum van ondertekening van het Convenant en eindigt automatisch door opzegging van het Convenant.

13.2 Het beëindigen van deze Verwerkersovereenkomst zal Verwerker niet ontslaan van haar vertrouwelijkheidsverplichtingen ingevolge artikel 3.

14. Overige bepalingen

14.1 Wijzigingen van deze Verwerkersovereenkomst zijn enkel van toepassing als deze door beide Partijen schriftelijk zijn geaccepteerd.

14.2 De Verwerkingsverantwoordelijke heeft aan de Regiegroep een onherroepelijke volmacht verleend om namens haar in te stemmen met wijzigingen van deze Verwerkersovereenkomst. Verwerkingsverantwoordelijke garandeert dat deze volmacht gedurende de looptijd van deze Verwerkersovereenkomst van kracht blijft en zal geen beroep doen op het ontbreken van een dergelijke volmacht.

14.3 Verwerker zal Verwerkingsverantwoordelijke desgevraagd bijstand verlenen bij het uitvoeren van een gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging van de Autoriteit Persoonsgegevens.

14.4 In het geval dat er een tegenstrijdigheid is tussen de bepalingen uit deze Verwerkersovereenkomst en de bepalingen van het Convenant of de Licentieovereenkomst, dan zullen de bepalingen van deze Verwerkersovereenkomst leidend zijn.

14.5 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing. Geschillen over of in verband met deze Verwerkersovereenkomst vallen onder de exclusieve rechtsmacht van de Rechtbank te Gelderland, locatie Zutphen.

Annex 1 bij Verwerkersovereenkomst

Politiegegevens in BRS worden slechts verwerkt voor de volgende doelen:

a) het houden van toezicht op naleving en handhaving van wetgeving door de Boa's binnen het kader van hun wettelijke opsporingstaken;
b) het opsporen van strafbare feiten door de Boa's binnen het kader van hun wettelijke opsporingstaken;
c) het verrichten van een concreet opsporingsonderzoek op verzoek van een officier van justitie;
d) het samenwerken met andere bevoegde opsporingsinstanties binnen het kader van hun wettelijke taken;
e) het samenstellen en op verzoek beschikbaar stellen van anonieme rapportages op basis van in BRS verwerkte gegevens;
f) het verstrekken van Politiegegevens conform de Verstrekkingenwijzer Wpg voor Boa's, vastgesteld overeenkomstig het Besluit en de Wpg en gepubliceerd in BRS, alsmede;
    i) het informeren van de (direct)toezichthouders, (het samenwerkingsverband van) de werkgever en de desbetreffende Boa indien er sprake is van een klacht gericht tegen het optreden van een Boa;
    ii) het verstrekken van gegevens uit BRS ten behoeve van beleidsinformatie, wetenschappelijk onderzoek en statistiek aan daartoe gekwalificeerde onderzoekers of onderzoeksinstituten.

In BRS worden daarnaast Persoonsgegevens verwerkt van Boa's en Persoonsgegevens van contactpersonen bij de Verwerkingsverantwoordelijke voor zover dit gegeven de onder a tot en met e genoemde doeleinden van Verwerken van Politiegegevens noodzakelijk is of noodzakelijk is voor het functioneren van technische voorzieningen, waaronder communicatievoorzieningen. In BRS kunnen Persoonsgegevens van Boa's worden verwerkt voor het faciliteren van communicatie tussen Boa's via beveiligde applicaties, en voor noodmeldingen alsmede voor operationele aansturing van Boa's.

Toelichting grondslagen

In dit document kunt u secties vinden die onleesbaar zijn gemaakt. Deze informatie is achterwege gelaten op basis van de Wet open overheid (Woo). De letter die hierbij is vermeld correspondeert met de bijbehorende grondslag in onderstaand overzicht.

J Art. 5.1 lid 2 sub e

Het belang van de openbaarmaking van deze informatie weegt niet op tegen het belang van de eerbiediging van de persoonlijke levenssfeer van betrokkenen

Overzicht Inbreuken in verband met persoonsgegevens (datalekken) 2022				
Kwartaal	**Nr.**	**Aard inbreuken**	**Toelichting**	**Melding bij de Autoriteit Persoonsgegevens (AP)**
Q1	1	Inbreuk op de vertrouwelijkheid	**Datalek** [redacted] Tijdens controle van de logbestanden is gebleken dat voorafgaand aan de verwijdering van de [redacted]-kwetsbaarheid uit [redacted] een verdachte activiteit heeft plaatsgevonden in [redacted]. **Genomen maatregelen:** • Forensisch onderzoek door het Nationaal Cyber Security Center (NCSC). Hieruit bleek dat er geen bewijs is dat er daadwerkelijk inbraak heeft plaatsgevonden in de systemen van Staatsbosbeheer.	Ja Aanvankelijk is uit voorzorg melding gemaakt bij de AP gelet op aard en omvang van de gegevensuitwisseling in [redacted]. Na Forensisch onderzoek en getroffen maatregelen is de melding bij de Autoriteit Persoonsgegevens weer ingetrokken.
	2.	Inbreuk op de vertrouwelijkheid	**Datalek DT-bestanden** Melding dat een map met DT-bestanden in het systeem [redacted] gedurende een bepaalde periode toegankelijk was voor onbevoegde interne gebruikers. **Genomen Maatregelen:** • Intern onderzoek naar oorzaak datalek. Hieruit bleek dat de stukken niet zijn geraadpleegd door onbevoegden. • Wijzigen autorisaties en controlemaatregelen getroffen om te voorkomen dat deze situatie zich weer voordoet.	Nee Gelet op de uitkomsten van intern onderzoek en genomen maatregelen is het onwaarschijnlijk dat het datalek een hoog risico oplevert voor de privacy rechten en vrijheden van degenen wiens persoonsgegevens toegankelijk waren.
Q2	3	Inbreuk op de vertrouwelijkheid	**Datalek fout distributielijst** Interne melding van onterecht ontvangen mailbericht. Dit blijkt veroorzaakt door het omzetten van Outlook distributielijsten naar de nieuwe Exchange Online omgeving met andere rollen/autorisaties. Hierdoor zijn meerdere e-mailberichten bij onbedoelde (interne) ontvangers terecht gekomen. De berichten bevatte geen gevoelige persoonsgegevens. **Getroffen maatregelen:** • Onderzoek naar oorzaak en omvang datalek.	Nee Gelet op de uitkomsten van intern onderzoek en genomen maatregelen is het onwaarschijnlijk dat het datalek een hoog risico oplevert voor de privacy rechten en vrijheden van degenen wiens persoonsgegevens mogelijk toegankelijk waren.

			• Controle en waar nodig aanpassing van alle interne e-mail distributielijsten. • Voorgenomen maatregel: jaarlijks de eigenaren van distributielijsten verzoeken om de lijsten te controleren en waar nodig aan te passen of op te heffen.	
	4	Inbreuk op de vertrouwelijkheid	**Datalek onjuist geadresseerde e-mail** Door gebruik van een onjuist distributielijst is een document bestemd voor beperkt intern gebruik breder binnen de organisatie verspreid. Het document bleek geen persoonsgegevens te bevatten anders dan de namen van de auteurs en de directeur. **Genomen maatregelen:** • Direct na verzending is de fout ontdekt en is de e-mail ingetrokken en de bijlagen verwijderd. • Degenen, die de mail al geopend hadden, zijn verzocht de bijlagen te verwijderen en niet verder te verspreiden.	Nee Gelet op aard en omvang en genomen maatregelen is niet waarschijnlijk geacht dat het datalek risico's oplevert voor betrokkenen.
	5	Inbreuk op de vertrouwelijkheid	**Datalek Cloud provider** Melding Datalek bij Cloud provider. Cloud provider heeft een afmelding Onderhoud verstuurd aan alle klanten en daarbij alle geadresseerden in de "AAN" i.p.v. in de "BCC" gezet.	N.v.t. Betreft datalek bij Cloudprovider. Deze leverancier heeft aangegeven dat gezien de mogelijk beperkte impact hier geen verdere opvolging aan te geven, anders dan opname in het interne incidentenregister.
	6	Inbreuk op de vertrouwelijkheid	**Datalek Cloud provider** ICT-team constateert dat in de log van de back-up gegevens staan van andere klanten van de Cloud provider. Na melding en onderzoek door de Cloudprovider blijkt dat er sprake is van fout in een script. De gegevens van Staatsbosbeheer(ders) zijn niet in files van andere klanten weggeschreven.	N.v.t. betreft datalek bij leverancier
	7	Inbreuk op de vertrouwelijkheid	**Datalek facturen** Melding door externe debiteur van ontvangst van 54 facturen	Ja Mede gelet op de hoeveelheid gegevens en

			bestemd voor andere klanten van Staatsbosbeheer (20 natuurlijke personen/ 29 rechtspersonen). Uit onderzoek bleek dat het datalek is veroorzaakt door onbewust menselijk handelen. Genomen maatregelen: • Incident is besproken in het werkoverleg • Onderzoek of automatische ondersteuning van het proces kan worden verbeterd.	feit dat het document in geautomatiseerd systeem van ontvanger terecht is gekomen en door meerdere medewerkers is ingezien, kan het risico op mogelijk onjuist gebruik niet geheel worden uitgesloten.
Q3	8	Inbreuk op de vertrouwelijkheid	**Datalek bij externe leverancier** Melding van datalek bij externe leverancier. Na onderzoek bleek dat de gegevens van andere klanten zijn getroffen en niet van Staatsbosbeheer(ders). Dit had te maken met verschillende bestelprocedures.	n.v.t. Betreft datalek bij externe leverancier. De leverancier heeft het datalek gemeld bij de Autoriteit Persoonsgegevens
	9	Inbreuk op de vertrouwelijkheid	**Datalek onjuist verstuurde e-mail** Abusievelijk onjuist adresseren van een interne mail aan de afdeling facilitair in plaats van aan de receptie met namen van 5 bezoekers. **Genomen maatregelen:** • Interne ontvanger (Facilitair) verzocht de mail te verwijderen, hetgeen is bevestigd. • Informeren betrokkenen.	Nee Gelet op geringe omvang en de aard van de gegevens en genomen maatregelen, is het niet waarschijnlijk dat het datalek een risico inhoudt voor degenen wiens gegevens zijn gelekt.
	10	Inbreuk op de vertrouwelijkheid en mogelijk inbreuk op de beschikbaarheid	**Datalek verplaatsen werkmap** Intern incident waarbij door (onbewust) menselijk handelen een gehele werkmap is verplaatst naar een directory van een ander team. **Genomen maatregelen:** • (Tijdelijk) intrekken autorisaties. • Terugplaatsen betreffende map middels een back-up.	Ja Ondanks dat niet is gebleken dat de gegevens daadwerkelijk door onbevoegden zijn ingezien, is het incident toch gemeld bij de Autoriteit Persoonsgegevens. Dit gelet op de aard en hoeveelheid van de gegevens die voor een korte periode toegankelijk waren voor onbevoegde interne medewerkers en gelet op het risico dat er recente informatie verloren is gegaan bij het terugplaatsen van de

				bestanden middels een back up.
Q4	11	Onbekend	**Extern gemeld datalek** Melding door burger dat er sprake zou zijn van een datalek bij Staatsbosbeheer. Intern onderzoek, w.o. navraag bij (software-) leveranciers, heeft niets opgeleverd. Ook melder kon geen nadere informatie verschaffen. Onderzoek afgerond daar er geen andere meldingen of signalen bekend waren over een incident. Melder is hiervan op de hoogte gesteld.	Nee Uit onderzoek is niet gebleken dat er daadwerkelijk sprake was van datalek.
	12	Inbreuk op de vertrouwelijkheid	**Datalek verkeerd verstuurde facturen** Melding door debiteur van ontvangst van een tweetal facturen bestemd voor andere debiteuren. Dit blijkt veroorzaakt door abusievelijk handmatig samenvoegen van facturen. De ontvanger is een betrouwbare zakenrelatie van Staatsbosbeheer en heeft direct na ontvangst melding gemaakt. **Genomen maatregelen:** • Onbevoegde ontvanger verzocht om onjuist ontvangen facturen te verwijderen, hetgeen bevestigd is. • Bespreking van het incident in betreffende team en opnieuw uitsturen van de facturen naar de juiste ontvangers.	Nee Gelet op de aard en omvang van gegevens en feit dat de ontvanger een betrouwbare zakenrelatie betreft, maakt het niet waarschijnlijk dat het datalek een risico inhoudt voor degenen wiens gegevens zijn gelekt.

Toelichting grondslagen

In dit document kunt u secties vinden die onleesbaar zijn gemaakt. Deze informatie is achterwege gelaten op basis van de Wet open overheid (Woo). De letter die hierbij is vermeld correspondeert met de bijbehorende grondslag in onderstaand overzicht.

N Art. 5.1 lid 2 sub i

Het belang van de openbaarmaking van deze informatie weegt niet op tegen het belang van het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen

Overzicht Inbreuken in verband met persoonsgegevens (datalekken) 2023				
Kwartaal	**Nr.**	**Aard inbreuken**	**Toelichting**	**Melding bij de Autoriteit Persoonsgegevens (AP)**
Q1	1	Risico op inbreuk op vertrouwelijkheid en inbreuk op de beschikbaarheid	**Datalek Nebu** Aanvankelijk melding vanuit NS naar alle reizigers, waaronder medewerkers van Staatsbosbeheer, dat er sprake is van een groot datalek bij de softwareleverancier Nebu. Vanuit TNO volgt de melding dat de software van Nebu is gebruikt voor de Werkgevers Enquête Arbeid (WEA) en dat een aantal organisatieonderdelen van Staatsbosbeheer deze Enquête hebben ingevuld. Op de vragenlijst zijn alleen bedrijfsgegevens en geen direct identificerende persoonsgegevens ingevuld. **Getroffen maatregelen:** • Op verzoek van het Ministerie van EZK/LNV (conform het Rijks brede advies) inventarisatie uitgevoerd binnen de organisatie in hoeverre de afgelopen jaren diensten zijn afgenomen van marktonderzoekspartijen, die gebruik maken van softwareleverancier Nebu. Uit intern onderzoek is niet gebleken dat de door Staatsbosbeheer ingeschakelde marktonderzoeksbureaus geraakt zijn door het datalek bij Nebu.	N.v.t. Betreft Datalek bij externe leveranciers/samenwerkingspartners van Staatsbosbeheer. Vanuit deze partijen is het datalek gemeld bij de Autoriteit Persoonsgegevens.
Q2	2.	Risico op inbreuk op de vertrouwelijkheid en inbreuk op de beschikbaarheid	**Datalek bij externe leverancier Tennet** Melding ten aanzien van datalek bij externe leverancier van Staatsbosbeheer Tennet. Datalek betreft hack van software. Tennet gebruikt deze software om bestanden uit te wisselen. Hierbij zijn gegevens van Staatsbosbeheer buitgemaakt (naam en IBAN-nummer organisatie en naam, handtekening en werklocatie adres van contactpersoon van SBB). **Getroffen maatregelen:** Betreffende medewerkers zijn geïnformeerd door/namens Tennet en geadviseerd alert te zijn op mogelijke phishingmail e-mails.	N.v.t. Betreft een datalek bij externe leveranciers/ samenwerkingspartner van Staatsbosbeheer. Vanuit betreffende partij is het datalek gemeld bij de Autoriteit Persoonsgegevens.

Q3	3	Risico op inbreuk op de vertrouwelijkheid en inbreuk op de beschikbaarheid	**Datalek** [redacted] Melding van een kwetsbaarheid in opensource software van welke in gebruik is bij een leverancier van Staatsbosbeheer. Uit onderzoek is niet gebleken dat de devices of data van Staatsbosbeheer geraakt zijn. **Getroffen maatregelen:** Op advies van de betreffende leverancier is de software op de Staatbosbeheer devices geüpdatet.	N.v.t.. Betreft data incident bij een externe leverancier van Staatsbosbeheer.
	4	Inbreuk op de vertrouwelijkheid	**Datalek Enquête Strandbad Maarsseveense Plassen** Melding van intern datalek. Betreft het versturen van een e-mail aan 425 abonnementhouders van een Strandbad met verzoek om een enquête in te vullen. Hierbij zijn abusievelijk alle e-mailadressen van de abonnementhouders vermeld stonden onder “aan” in plaats van onder “bcc”. Gevolg is dat de ontvangers van het bericht de e-mailadressen van de andere abonnementhouders hebben kunnen inzien. **Getroffen Maatregelen:** • Een mail naar alle geadresseerden op 29-08-2023 met informatie over en excuses voor het voorval, verzoek om e-mail te verwijderen en mededeling dat voorval zal worden gemeld bij AP en vermelding contactgegevens SBB voor eventuele vragen. • Proceseigenaar is door de privacy adviseurs geadviseerd over maatregelen om dergelijke voorvallen in de toekomst te voorkomen.	Ja De inbreuk in verband met persoonsgegevens is gemeld bij de Autoriteit Persoonsgegevens.
	5	Inbreuk op de vertrouwelijkheid	**Datalek lijst Senioren dag** Betreft het per abuis verzenden van een Excel lijst naar 125 deelnemers van de jaarlijkse ontmoetingsdag voor oud-medewerkers van Staatsbosbeheer. De Excel lijst bevatte NAW-gegevens en het geslacht (heer/mevrouw) van ongeveer 800 voormalig Staatsbosbeheer, voornamelijk gepensioneerden. De lijst bevatte ongeveer 98 telefoonnummers en 131 e-mailadressen van een aantal voormalig medewerkers. Van 12 personen bevat de lijst (gevoelige) persoonlijke informatie omtrent de	Ja Inbreuk in verband met persoonsgegevens is gemeld bij de Autoriteit Persoonsgegevens.

			reden van afwezigheid. Deze informatie is door/namens betrokkenen doorgeven. **Getroffen maatregelen:** • E-mail aan de 125 ontvangers van de Excel lijst met excuses en verzoek Excel lijst te verwijderen en niet te gebruiken/verspreiden en verwijdering van gegevens te bevestigen; • Brief aan overige betrokkenen (ongeveer 670 personen) met excuses en informatie over datalek, de genomen maatregelen en contactgegevens voor vragen; • Proceseigenaar geadviseerd over de te nemen maatregelen om dergelijke voorvallen in de toekomst te voorkomen.	
Q4	6	Risico op inbreuk op vertrouwelijkheid	**Datalek Phishingmail** Melding dat er een phishingmail is verstuurd uit naam van een van de directieleden. Vooralsnog is niet gebleken dat er data verloren is gegaan of gelekt is: geen aanleiding voor melding bij AP. **Getroffen maatregelen:** • Bericht geplaatst op intranet om medewerkers van Staatsbosbeheer te informeren en instrueren hoe te handelen bij ontvangst van phishingmail: de e-mail meteen verwijderen en indien geopend wachtwoord z.s.m. wijzigen.	Nee Tot op heden is niet gebleken dat er data verloren is gegaan of persoonsgegevens zijn gelekt. Gelet hierop geen aanleiding voor melding bij AP.

Toelichting grondslagen

In dit document kunt u secties vinden die onleesbaar zijn gemaakt. Deze informatie is achterwege gelaten op basis van de Wet open overheid (Woo). De letter die hierbij is vermeld correspondeert met de bijbehorende grondslag in onderstaand overzicht.

N Art. 5.1 lid 2 sub i

Het belang van de openbaarmaking van deze informatie weegt niet op tegen het belang van het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen

Overzicht Meldingen (mogelijke) inbreuken in verband met persoonsgegevens (datalekken) 2024				
Kwartaal	**Nr.**	**Aard inbreuken**	**Toelichting**	**Melding bij de Autoriteit Persoonsgegevens (AP)**
Q1 (jan)	1	Risico op inbreuk op Vertrouwelijkheid en inbreuk op de beschikbaarheid	**Melding gestolen werktelefoon** De melding is door team Facilitair afgehandeld. **Genomen maatregelen:** • Simkaart geblokkeerd; • Nieuwe telefoon met nieuwe simkaart uitgereikt.	Nee Gelet op de genomen maatregelen en er geen aanwijzingen waren/zijn dat er toegang is verkregen tot het account van de medewerker is geen aanleiding gezien om het datalek te melden bij de AP.
(Jan)	2	Risico op inbreuk op Vertrouwelijkheid	**Melding datalek Woo-verzoek** Bij de afhandeling van een Woo-verzoek is een e-mail ter informatie naar de betreffende teamleider gestuurd met in de tekst van de e-mail en in het besluit de naam van indiener van het verzoek. Dit had geanonimiseerd moeten worden verzonden. Informatie is intern gebleven. **Genomen maatregelen:** • Teamleider is verzocht om de e-mail met bijlagen te verwijderen.	Nee Betreft een betrouwbare ontvanger en informatie is intern gebleven, waardoor het niet aannemelijk is dat het datalek een (hoog) risico inhoudt voor betrokkene.
(Feb)	3	Risico op inbreuk op vertrouwelijkheid	**Melding phishing mail** Twee medewerkers van SBB hebben bij ICT-melding gemaakt van de ontvangst van een “verdachte mail” afkomstig van een G-mail-adres van een collega. Het bleek om een phishing mail te gaan. **Getroffen maatregelen:** • N.a.v. de melding heeft Microsoft de spamfilter aanpast o.b.v. de inhoud van de berichten. • De “verdachte mails” zijn naar de junk folder verplaatst waarna de meldingen door ICT zijn afgesloten.	Nee Doordat de medewerkers alert hebben gehandeld hebben de phishingmails niet tot een datalek geleid.
(Mrt)	4	Risico op inbreuk op vertrouwelijkheid	**Melding te breed ingestelde autorisaties archiefsysteem** In het kader van het bijwerken van het register van verwerkingen is ten aanzien van een specifieke verwerking een controle verricht in het archief systeem [redacted]. Hierbij bleek dat (kopie) identiteitsbewijzen inzichtelijk waren voor eenieder binnen de organisatie,	Nee Betreft kwetsbaarheid in beveiliging. Tot op heden geen signalen dat er daadwerkelijk gebruik is gemaakt van de kwetsbaarheid.

			terwijl dit niet voor eenieder noodzakelijk is voor de werkzaamheden. **Getroffen maatregelen:** • Onderzoek omvang kwetsbaarheid; • Onderzoek noodzaak verwerking; • (Start met) beperken rechten daar waar nodig; • Aanpassen proces/werkinstructie; • Inzet op versterken bewustwording binnen het team dat verantwoordelijk is voor de verwerking en meenemen in bewustwordingscampagne voor gehele organisatie vanuit DIV/ICT en Privacy;	Gelet op de ingang gezette maatregelen en de resultaten van het onderzoek is vooralsnog niet aannemelijk dat de kwetsbaarheid een (hoog) risico inhoudt voor betrokkenen. De kwetsbaarheid is opgenomen in het interne AVG-inbreuken register en de voortgang van de maatregelen worden gemonitord.
Q2 (apr)	5	Risico op inbreuk op de vertrouwelijkheid en inbreuk op de beschikbaarheid	**Melding twee gestolen laptops** Bij een inbraak in een werkschuur zijn onder meer 2 laptops gestolen. **Getroffen maatregelen:** • Wijzigen account/ wachtwoorden; • Opdracht tot wissen op afstand. • Advies heroverwegen MFA voor devices waar dat nog niet voor ingeregeld is.	Ja Door het ontbreken van een Multifactor authenticatie (MFA) op de laptops kan niet worden uitgesloten dat kwaadwillenden toegang hebben gehad tot (persoons-) gegevens. Gelet hierop is het incident tijdig gemeld bij de Autoriteit Persoonsgegevens.
(Mei)	6	Risico op inbreuk op de vertrouwelijkheid	**Melding bestanden naar verkeerd extern e-mailadres verstuurd** In het kader van de afhandeling van een WOO-verzoek zijn geanonimiseerde bestanden verstuurd zijn aan het “verkeerd” extern emailadres. De verkeerde adressering kwam doordat er blijkbaar twee organisaties met exact dezelfde naam bestaan. **Getroffen maatregelen:** • Ontvanger is gevraagd om de e-mail met bijlagen te verwijderen ondanks dat het geanonimiseerde stukken betrof die openbaar werden gemaakt. Aan dat verzoek is dezelfde dag nog gehoor gegeven.	Nee Geen datalek/niet aannemelijk dat er een risico bestaat voor betrokkenen omdat de bestanden geanonimiseerd verstuurd zijn.

(Jun)	7	Risico op inbreuk op de vertrouwelijkheid	**Melding malware gedetecteerd en verspreid** Een medewerker van Staatsbosbeheer heeft een e-mail ontvangen van een zakelijke relatie met een link naar een bestand op OneDrive. De medewerker was in afwachting van een bericht van de zakelijke relatie en heeft niets vermoedend op de link geklikt. De e-mail bleek malware te bevatten en het klikken op de link heeft een zogenoemde e-mailbom geactiveerd. Dit heeft geresulteerd in het versturen van malware naar 111 zakelijke relaties van de SBB-medewerker. De e-mail bleek moeilijk te herkennen als spam/phishingmail. **Getroffen maatregelen:** • Wijzigen wachtwoord; • Informeren van de 111 geadresseerden met verzoek niet te klikken op de link in de ontvangen e-mail en de e-mail te verwijderen.	Ja Toegang door kwaadwillenden tot OneDrive kon niet geheel uitgesloten worden. Gelet hierop is het incident gemeld bij de AP.
(Jun)	8	Inbreuk op de vertrouwelijkheid	**Melding te breed ingestelde autorisatie financieel systeem** Melding is afkomstig van een medewerker van Staatsbosbeheer die bij het invoeren van een zoekopdracht naar leveranciers in het financiële systeem van Staatsbosbeheer de namen en privéadressen van collega's, stagiaires en vrijwilligers te zien kreeg. Het leek erop dat de betreffende collega de toegang tot al deze gegevens niet nodig heeft voor de uitoefening van haar werkzaamheden en er mogelijk sprake is van te breed ingesteld toegangsrechten/autorisaties. **Getroffen Maatregelen:** • Onderzoek naar ingestelde toegangsrechten/autorisaties; • Controle in hoeverre huidige autorisatiematrix volstaat; • Naar aanleiding van onderzoek opstellen plan van aanpak herinrichting autorisaties/toegangsrechten en/of aanvullende maatregelen genomen moeten worden en welke dit dan zijn.	Nee Omdat hier sprake is van een betrouwbare ontvanger/melder is vooralsnog niet aannemelijk dat de kwetsbaarheid een (hoog) risico inhoudt voor betrokkenen. Gelet hierop en op de geplande en reeds in gang gezette maatregelen is vooralsnog geen aanleiding gezien om de kwetsbaarheid te melden bij de AP. Voortgang van de (voorgenomen) maatregelen worden gemonitord.

			• Start met inregelen benodigde maatregelen;	
Q3 (jul)	9	Risico op inbreuk op de vertrouwelijkheid en inbreuk op de beschikbaarheid	**Melding mogelijke hack telefoon** Betreft melding mogelijke hack van een telefoon. Het toestel voerde uit zichzelf acties uit (‘ghost touches’) in de NS Reisplanner. Tevens bleken alle e-mails verzonden in de week voorafgaand aan het incident te zijn verdwenen uit het outlookaccount. De telefoon is voor forensisch onderzoek opgestuurd naar het Nationaal Cyber Security Center (NCSC). Het NCSC heeft geen misbruik van het toestel geconstateerd en geen aanwijzingen dat er een datalek heeft plaatsgevonden. Mogelijk ligt de oorzaak in een defect in de oplaadkabel. **Getroffen Maatregelen:** • Wachtwoord account gewijzigd; • Nieuwe telefoon met nieuwe simkaart uitgegeven; • Verdwenen e-mails teruggezet in mailbox; • Telefoon laten onderzoeken door NCSC.	Ja Gelet op de kwaadaardige aard van een hack is op een voorlopige melding gemaakt bij de AP. Gelet op uitkomsten van het onderzoek door het NCSC is de datalekmelding bij de AP op 28/8 ingetrokken.
(Aug)	10	Risico op inbreuk op vertrouwelijkheid en inbreuk op de beschikbaarheid	**Melding geslaagde phishing poging** De ontvangen e-mail was verstuurd uit naam van een externe relatie aan 4 Staatsbosbeheer medewerkers en bevatte een link naar Dropbox. Een van de collega’s verwachtte een bericht van degene uit wiens naam de mail leek te zijn gestuurd en heeft op de link geklikt en credentials ingevuld. De collega kreeg argwaan en heeft contact opgenomen met de vermoedelijke afzender, waarna bleek dat het om phishingmail ging. Uit onderzoek blijkt dat diezelfde dag een succesvolle inlog is geweest vanuit de VS en onbevoegden toegang hebben gehad tot de persoonlijke Microsoft 365 omgeving van de collega. Uit logbestanden blijkt niet dat er bestanden zijn geopend of applicaties zijn gestart. Wel zijn persoonsgegevens (zakelijke contactgegevens) zichtbaar geweest. **Getroffen maatregelen:**	Ja inbreuk is tijdig gemeld bij de Autoriteit Persoonsgegevens.

			• Tijdelijk blokkeren van accounts en wijzigen wachtwoorden; • Aanpassen Microsoft-inlogpagina SBB zodat deze beter herkenbaar is en het risico op inloggen op een neppagina wordt verkleind; • Bericht op Digitalis over aanpassing inlogpagina+ algemene info over het herkennen van en handelen bij Phishing; • E-mail aan alle betrokken om hen te informeren en te adviseren alert te zijn. • Bericht op Digitalis specifiek over dit datalek ter informatie/waarschuwing en verhogen van Awareness. **Toekomstige maatregelen:** • 2e helft 2024: heroverwegen inregelen Multifactor authenticatie (MFA) voor alle mobiele devices;	
(Sept)	11	Inbreuk op de vertrouwelijkheid	**Melding datalek namen sollicitanten** Een extern ingehuurd wervingsbureau heeft in een uitnodiging aan de selectiecommissie de namen van twee eindkandidaten vermeld. De agenda's van de commissieleden in dienst bij Staatsbosbeheer zijn inzichtelijk voor alle collega's van Staatsbosbeheer en daarmee ook de betreffende uitnodiging. In hoeverre de afspraak in de agenda's daadwerkelijk door Staatsbosbeheer collega's is geraadpleegd is niet bekend/ gelogd. **Getroffen maatregelen:** • Direct na het ontdekken van het incident zijn de afspraken in de agenda afgeschermd; • Het externe wervingsbureau is verzocht om een toelichting te geven op de gehanteerde werkwijze en aan te geven op welke wijze het bureau omgaat met de situatie richting de betrokkenen; • Betreffende commissieleden zijn geadviseerd om in het vervolg gevoelige c.q. vertrouwelijke gegevens direct na ontvangst af te schermen.	Nee Gelet op de korte duur dat de gegevens inzichtelijk waren, de aard van het datalek en de aard van de gegevens en de genomen maatregelen is het onwaarschijnlijk dat het datalek een hoog risico oplevert voor de privacy rechten en vrijheden van degenen wiens persoonsgegevens toegankelijk waren.
Q4 (okt)	12	Inbreuk op de vertrouwelijkheid	**Melding datalek gebruik ChatGPT** Een medewerker heeft voor de afhandeling van correspondentie de tekst van een e-mail gekopieerd naar	Nee Gelet op de aard en beperkte hoeveelheid van de gelekte gegevens

			ChatGPT waarbij abusievelijk de persoonsgegevens van de afzender van de e-mail niet zijn verwijderd uit de prompt. **Getroffen maatregelen:** • Opstellen en publiceren richtlijnen gebruik generatieve AI op Digitalis.	en de zeer geringe kans dat deze zichtbaar worden voor andere gebruikers van ChatGPT is het niet waarschijnlijk dat het datalek een (hoog) risico oplevert voor de rechten en vrijheden van betrokkene.
(Nov)	13	Risico op inbreuk op vertrouwelijkheid	**E-mail verzonden aan onjuist geadresseerde** Per abuis is een boekingsbevestiging verstuurd aan de verkeerde persoon. Betrof naam, e-mail en telefoonnummer. De onjuiste ontvanger heeft het datalek gemeld en op verzoek van Staatsbosbeheer de e-mail verwijderd. Betreft 1 e-mail met beperkte gegevens. **Getroffen maatregelen:** • Ontvanger verzocht e-mail te verwijderen; • E-mail opnieuw uitgestuurd naar juiste ontvanger; • Informeren betrokkene;	Nee Gelet op de aard van het datalek/de beperkte gegevens en het feit dat ontvanger direct melding heeft gemaakt en bevestigd heeft de e-mail te hebben verwijderd is het onwaarschijnlijk dat het datalek een hoog risico oplevert voor de privacy rechten en vrijheden van betrokkene.
(Dec)	14	Risico op inbreuk op vertrouwelijkheid en inbreuk op de beschikbaarheid	**Poging tot Smishing** Melding is afkomstig van een medewerker van Staatsbosbeheer, die niet lang na inhouding van een verkeersboete op zijn salaris, een betalingsherinnering ontving van een onbekend telefoonnummer. Na onderzoek blijkt het om poging tot sms-phishing (smishing) te gaan. De medewerker heeft niet op de link geklik waardoor geen gegevens zijn gelekt. Uit navraag blijkt dat de overige collega’s, die recent een verkeersboete hebben ontvangen, er tot nog toe niet één eenzelfde sms heeft ontvangen.	Nee betrokkene heeft niet op link geklikt waardoor verder geen gegevens zijn gelekt.

Toelichting grondslagen

In dit document kunt u secties vinden die onleesbaar zijn gemaakt. Deze informatie is achterwege gelaten op basis van de Wet open overheid (Woo). De letter die hierbij is vermeld correspondeert met de bijbehorende grondslag in onderstaand overzicht.

N Art. 5.1 lid 2 sub i

Het belang van de openbaarmaking van deze informatie weegt niet op tegen het belang van het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen

Overzicht Meldingen (mogelijke) inbreuken in verband met persoonsgegevens (datalekken) 2025				
Kwartaal	**Nr.**	**Aard inbreuken**	**Toelichting Melding**	**Melding bij de Autoriteit Persoonsgegevens (AP)**
Q1 (Jan)	1	Risico op inbreuk op Vertrouwelijkheid en inbreuk op de beschikbaarheid	**Melding vermissing Smartphone** Betreft vermissing werktelefoon tijdens externe bijeenkomst. Telefoon was voorzien van een pincode. **Genomen maatregelen:** • Wachtwoord SBB-account gewijzigd; • Opdracht tot wissen SBB-profiel. NB. Het daadwerkelijk wissen van het profiel vindt plaats zodra telefoon verbinding maakt met internet.	Nee Twee dagen later heeft melder laten weten dat het toestel weer terecht is.
(Feb)	2	Risico op inbreuk op Vertrouwelijkheid en inbreuk op de beschikbaarheid	**Datalek Inzage persoonlijke map collega** Melding van een medewerker dat hij via zijn OneDrive toegang heeft tot een map met persoonlijke documenten van een collega. Om privacy redenen is (in afstemming met betrokkene) beperkt technisch onderzoek uitgevoerd. Op basis van dit onderzoek kon de precieze oorzaak van het datalek niet worden vastgesteld. **Genomen maatregelen:** • Map met persoonlijke data is verwijderd uit de persoonlijke map van de melder en in de persoonlijke map van betrokkene geplaatst; • Betrokkene is geïnformeerd;	Ja Ondanks dat sprake is van een betrouwbare ontvanger, is het datalek gemeld bij de AP. Dit gelet op de aard en gevoeligheid van de persoonsgegevens en het feit dat onderzoek niet heeft uitgewezen wat de precieze oorzaak van het datalek is.
(Feb)	3	Risico op inbreuk op vertrouwelijkheid	**Datalek onjuist geadresseerde e-mail** Medewerker stuurt e-mail met persoonsgegevens (voornamen en geplande inzet uren voor project) in plaats van naar een collega naar een medewerker van een provincie met nagenoeg dezelfde achternaam. De onbevoegde ontvanger maakt hiervan direct melding. **Genomen maatregelen:** • Onbevoegde ontvanger verzocht om de e-mail te verwijderen, hetgeen is bevestigd.	Nee Aannemelijk is dat hier sprake is van een betrouwbare ontvanger/melder. Mede gelet op de aard en beperkte hoeveelheid gelekte persoonsgegevens is het aannemelijk dat het datalek geen (hoog) risico inhoudt voor betrokkenen. Gelet hierop is het datalek niet gemeld bij de AP.
(Mrt)	4	Risico op inbreuk op vertrouwelijkheid	**Melding onjuist geadresseerde Arbo-melding**	Nee

			Datalek veroorzaakt bij het invullen van een nieuw digitaal formulier voor ARBO- incidenten. Gebleken is dat bij de ontwikkeling van het formulier per abuis een verkeerd account/e-mailadres is gekozen voor de automatische verwerking van formulier. De onbevoegde ontvanger, een medewerker van een gemeente, heeft hiervan direct melding gemaakt. **Getroffen maatregelen:** - Onbevoegde ontvanger verzocht e-mail te verwijderen, hetgeen ontvanger heeft bevestigd. - Foutieve e-mailadres verwijderd uit digitaal meldformulier. - Betrokkene geïnformeerd over datalek.	Aannemelijk is dat hier sprake is van een betrouwbare ontvanger/melder. Gelet hierop is aannemelijk dat het datalek geen (hoog) risico inhoudt voor betrokkenen.