Omgevingsdienst Zuid-Holland Zuid

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 953

12 november 2021

Officiële uitgave van de gemeenschappelijke regeling Omgevingsdienst Zuid-Holland Zuid

Addendum Privacybeleid OZHZ vanwege de Wet politiegegevens

1. Inleiding

Vanaf 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG). De Omgevingsdienst Zuid-Holland Zuid (OZHZ) heeft in zijn privacybeleid en informatiebeveiligingsbeleid vastgelegd hoe hij omgaat met de bescherming van persoonsgegevens. De verwerking van persoonsgegevens moet zorgvuldig, rechtmatig en veilig plaatsvinden. Veel informatie is te vinden op de website van OZHZ: www.ozhz.nl/privacy.

De verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren (boa's) valt niet onder de AVG maar onder de Wet politiegegevens (Wpg). Daarnaast is een aantal andere regelingen van toepassing op de verwerking van politiegegevens. Zoals het Besluit politiegegevens (Bpg), het Besluit politiegegevens buitengewoon opsporingsambtenaren en de Regeling periodieke audit politiegegevens. OZHZ heeft ongeveer 12 boa's in dienst en is als werkgever 'verwerkingsverantwoordelijke' in het kader van de Wpg.

De AVG en de Wpg sluiten elkaar wederzijds uit. Op een aantal onderdelen is zeker ook sprake van overlap. Andere verplichtingen zijn vergelijkbaar maar kennen verschillen in de concrete uitwerking, zoals de verplichting voor de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen te treffen ter bescherming en beveiliging van de gegevens. In het kader van de Wpg is bijvoorbeeld ook eens per 4 jaar een externe audit verplicht en moeten elk jaar interne audits worden gehouden.

Het huidige privacybeleid van OZHZ gaat alleen uit van de AVG. Het is daarom wenselijk er de verplichtingen uit de Wpg aan toe te voegen.

2. De boa's bij OZHZ

Omgevingsdiensten zijn op grond van de 'Kwaliteitscriteria voor vergunningverlening, toezicht en handhaving krachtens de Wabo', criterium 12, verplicht om boa's in dienst te hebben ten behoeve van de strafrechtelijke handhaving van de omgevingswet- en regelgeving, in het bijzonder op het taakveld milieu. Het is voor omgevingsdiensten op grond van artikel 5.4 van de Wet algemene bepalingen omgevingsrecht en de betreffende verordeningen van de gemeenten en provincie verplicht om hieraan uitvoering te geven. Naast deze verplichte milieu-boa's heeft OZHZ ook boa's in dienst die zich richten op de naleving van de groene wet- en regelgeving.

De boa's in dienst bij OZHZ vallen onder het zogenoemde domein II: Milieu, welzijn en infrastructuur. Zij zijn bevoegd processen-verbaal uit te schrijven en, namens de directeur van OZHZ, bestuurlijke strafbeschikkingen milieu op te leggen. In de 'Beleidsregel Toepassing Bestuurlijke strafbeschikking directeur Omgevingsdienst Zuid-Holland Zuid' is het geldende handhavingsbeleid ter zake opgenomen. Als beleid voor toepassing van de bestuurlijk strafbeschikking geldt:
- Het beleid, zoals vastgelegd in de geldende Landelijke Handhavingstrategie, en
- Het beleid, zoals vastgelegd in de 'Richtlijn bestuurlijke strafbeschikkingsbevoegdheid milieu- en keurfeiten (art. 257ba, tweede lid, Sv)'.

De directeur rapporteert elk jaar aan het AB over de toepassing van deze beleidsregel.

De boa's van OZHZ verwerken politiegegevens ten behoeve van de uitvoering van de politietaak als bedoeld in de artikelen 8 (de dagelijks politietaak), 9 (o.a. onderzoeken waarbij bijzondere opsporingsbevoegdheden worden ingezet, zoals het plaatsen van een baken onder een auto bij verdenking van stroperij of stelselmatige observatie bij verdenking van een milieudelict; na instemming van de bevoegd functionaris) en 13 (ondersteunende taken; dit artikel biedt de mogelijkheid om gegevens die oorspronkelijk zijn verwerkt op basis van artikel 8 of 9 verder te verwerken, bijvoorbeeld voor het raadplegen van pv's, boetes of overtredingen van gebiedsverboden voor alle opsporingsambtenaren in Nederland.) van de Wpg. Afhankelijk van de grondslag gelden er andere voorwaarden, bijvoorbeeld voor de verwerkingstermijn en toegankelijkheid voor andere opsporingsambtenaren. Het overgrote merendeel van de verwerkingen van een boa valt overigens onder artikel 8 van de Wpg.

OZHZ neemt geen besluiten die uitsluitend zijn gebaseerd op geautomatiseerde verwerking, als bedoeld in de Wpg. Ook vergelijkt OZHZ politiegegevens niet geautomatiseerd met andere politiegegevens.

3. Doelstellingen van het privacybeleid

Het privacybeleid van OZHZ beschrijft hoe de dienst verantwoordelijk en binnen wettelijke kaders met persoonsgegevens omgaat. Voor de reikwijdte van dit addendum bestaat het wettelijk kader voor bescherming van persoonsgegevens uit de Wpg en de genoemde regelingen. OZHZ implementeert de verplichtingen uit die wet- en regelgeving op zorgvuldige wijze. De boa's van OZHZ zijn zich ervan bewust dat zij zorgvuldig moeten omgaan met politiegegevens. Zij worden daarin getraind en er gelden interne werkinstructies hoe om te gaan met politiegegevens. Het geautomatiseerde systeem waarmee zij politiegegevens verwerken dwingt af dat de verwerking op rechtmatige wijze plaatsvindt.

OZHZ wil met dit addendum op het privacybeleid onder andere bereiken dat de boa's:
- Zich ten volle bewust zijn van de noodzaak om zorgvuldig en op rechtmatige wijze om te gaan met politiegegevens.
- De rechten van betrokkenen respecteren en werken volgens de vastgestelde procedures.
- Het vertrouwen van betrokkenen in de overheid niet beschamen.
- Gedrag vertonen dat past bij goed werknemerschap.
- De kans op financiële en imagoschade minimaliseren.

4. Juridisch kader

Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkenen voorop. Onnodige of te verregaande inbreuken moeten worden voorkomen. De AVG regelt het algemene kader voor de omgang met persoonsgegevens binnen de landen van de Europese unie. De uitgangspunten van de AVG zijn als volgt:
- Verwerking van persoonsgegevens vindt plaats op rechtmatige, behoorlijke en transparante wijze.
- Verwerking van persoonsgegevens mag alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.
- Verwerking van persoonsgegevens mag alleen op een van de in de AVG opgenomen grondslagen.
- Alleen de persoonsgegevens die voor het beoogde doel noodzakelijk zijn mogen worden verwerkt.
- Persoonsgegevens moeten juist zijn en blijven.
- Persoonsgegevens mogen niet langer bewaard worden dan nodig voor het beoogde doel.
- Persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging.
- OZHZ moet als verwerkingsverantwoordelijke kunnen aantonen aan deze regels te voldoen.

Het normenkader van de Wpg is grotendeels gelijkluidend aan dat van de AVG. Op hoofdlijnen geldt aanvullend nog het volgende:
- De boa's van OZHZ kunnen naast hun opsporingstaken ook bestuursrechtelijke toezichts- en handhavingstaken hebben. Zij krijgen dan bij het verwerken van persoonsgegevens te maken zowel met de AVG te maken als met de Wpg. In de verwerking van gegevens moet duidelijk zijn welke gegevens er worden verwerkt onder de AVG en welke onder de Wpg. De boa's van OZHZ doen dit door gebruik te maken van het Boa Registratie Systeem (hierna: BRS). Er worden in principe geen politiegegevens verwerkt buiten het BRS. De milieu-boa's die tevens toezichthouder zijn verwerken hun bestuurlijke toezichtsgegevens in het VTH-systeem van OZHZ. De groene boa's die tevens toezichthouder zijn doen dat in het Toezicht Registratiesysteem (TRS). Wanneer wordt vastgesteld dat sprake is van een strafrechtelijke overtreding schakelt TRS over naar BRS.
- De Wpg stelt andere eisen aan de verwerking van persoonsgegevens dan de AVG. Zo geldt onder andere de plicht tot delen met ieder andere opsporingsambtenaar die deze gegevens nodig heeft voor zijn werk (zowel alle boa's als algemene opsporingsambtenaren werkzaam bij de politie). Daartoe hebben de gebruikersorganisaties van het BRS in een convenant afspraken gemaakt over de wijze waarop politiegegevens worden verwerkt en uitgewisseld. Dit is vastgelegd in het Samenwerkingsverband uitwisseling politiegegevens BRS (SupBRS). Het SupBRS heeft afspraken gemaakt met de externe verwerker, NatuurNetwerk B.V., en een website ingericht waar betrokkenen informatie over BRS kunnen vinden (www.privacyvragenbrs.nl). Het Ministerie van Veiligheid en Justitie is sinds 2015 betrokken bij het SupBRS.

De hierna genoemde verplichtingen uit de Wpg zijn veelal geborgd binnen het BRS:
- Er moet een scheiding worden aangebracht tussen gegevens die op feiten zijn gebaseerd en feiten die op een persoonlijk oordeel zijn gebaseerd.
- Er moet onderscheid worden gemaakt tussen betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden.
- Documentatie is vereist van de doelen van onderzoeken, verstrekking of doorgifte, afwijzing van verzoeken om inzage, inbreuk op de beveiliging, doorgifte buiten de EU met datum en tijd, ontvanger, redenen en doorgegeven gegevens en melding van gemeenschappelijke verwerkingen aan de Autoriteit Persoonsgegevens (AP).

- Er vindt logging plaats in geautomatiseerde systemen van de invoer van gegevens in systemen en op termijn ook van het verzamelen, wijzigen, raadplegen, verstrekken (o.a. in de vorm van doorgifte), combineren of vernietigen van politiegegevens.
- Er worden specifieke eisen gesteld aan de informatiebeveiliging uit het Bpg.
- Er gelden specifieke termijnen voor het bewaren, verwijderen en vernietigen van politiegegevens.
- Er geldt met ingang van 2021 een verplichting tot het uitvoeren van een externe privacyaudits. De rapportage die hieruit voortvloeit moet worden verstrekt aan de AP. Als er tekortkomingen zijn geconstateerd moet 3 maanden na het uitvoeren van de audit een verbeterrapport worden opgesteld, waarop binnen een jaar een hercontrole plaatsvindt. De hercontrole geldt alleen voor die onderdelen van de wet waar de tekortkomingen geconstateerd worden. De resultaten van de hercontrole worden vastgelegd in een rapportage en eveneens verstrekt aan de AP, uiterlijk 1 jaar na het uitvoeren van de externe audit.

Tot slot kan nog worden gewezen op de volgende verplichtingen:
- Inrichting van processen en systemen moet plaatsvinden volgens de principes van gegevensbescherming door beveiliging en ontwerp, gegevensbescherming door standaardinstellingen.
- Er gelden deels specifieke eisen voor de uitvoering van Data Protection Impact Assessments (DPIA's).
- Er geldt een plicht om een register van verwerkingen bij te houden, met daarin, aanvullend op de in de AVG gevraagde informatie, het bestaan van profilering, de categorieën van gegevens die worden doorgegeven buiten de EU, de grondslag, de toekenning van autorisaties.
- Het melden van datalekken, voorafgaande raadpleging van de AP en het benoemen van een Functionaris Gegevensbescherming.

5. Register van verwerkingen

Net als de AVG verplicht de Wpg tot het bijhouden van een register van verwerkingen. Wel zijn er enkele verschillen die hierna met een (*) zijn aangeduid. Het register van verwerkingen in het kader van de Wpg moet het volgende bevatten:
- De naam en de contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming.
- De doelen van de verwerking.
- De categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties.
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens.
- In voorkomend geval: het gebruik van profilering. (*)
- In voorkomend geval: de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie.
- Een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn. (*)
- Zo mogelijk: de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd.
- Zo mogelijk: een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging.
- De toekenning van de autorisaties. (*)

Het register van verwerkingen van OZHZ staat op www.ozhz.nl/privacy.

6. Verwerkersovereenkomsten

Een verwerker is een derde partij die in opdracht van de verwerkersverantwoordelijke persoonsgegevens verwerkt. Bij veel processen van overheidsorganisaties worden gegevens verwerkt door derden. Zo heeft OZHZ verwerkersovereenkomsten afgesloten voor de software ten behoeve van de uitvoering van VTH-taken, van het document managementsysteem en van het HRM-systeem (cloudapplicaties) en voor de dienstverlening door het Servicecentrum Drechtsteden (na 1 januari 2022 de servicegemeente Dordrecht).

Specifiek voor de taakuitvoering van de boa's van OZHZ kunnen hier worden genoemd de verwerkersovereenkomsten met NatuurNetwerk B.V. inzake het BRS en met het Centraal Justitieel Incasso Bureau.

In deze verwerkersovereenkomsten moet ten minste het volgende worden opgenomen (artikel 6:1b van het Bpg):
- Het onderwerp en de duur van de verwerking.
- De aard en het doel van de verwerking.
- Het soort gegevens waarop de wet van toepassing is.
- De categorieën van betrokkenen en de verplichtingen en de rechten van de verwerkingsverantwoordelijke.

Met name moet in de verwerkersovereenkomst zijn opgenomen dat de verwerker uitsluitend volgens de instructies van de verwerkingsverantwoordelijke handelt, er zorg voor draagt dat de tot het verwerken van politiegegevens gemachtigde personen zich ertoe hebben verplicht vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting daaraan gebonden zijn, de verwerkingsverantwoordelijke met passende middelen bijstaat om naleving van de bepalingen betreffende de rechten van de betrokkene te verzekeren, na afloop van de gegevensverwerkingsdiensten, naargelang de keuze van de verwerkingsverantwoordelijke, alle gegevens wist of hem deze ter beschikking stelt, en bestaande kopieën verwijdert, tenzij opslag van die gegevens verplicht is, de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om nakoming van in dit artikel gestelde voorschriften aan te tonen en aan de in dit artikel gestelde voorschriften voldoet bij de inschakeling van een andere verwerker en bij die inschakeling overeenkomstig artikel 6c, vierde lid, van de wet, handelt.

7. Informatiebeveiligingsbeleid

Het dagelijks bestuur stelde op 13 november 2020 het Strategisch Informatiebeveiligingsbeleid 2020-2024 vast. De basis voor dit beleid is de NEN-ISO/IEC 27001:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid, de BIO (als opvolger van de baseline informatiebeveiliging gemeenten, de BIG). Het is een richtinggevend en kaderstellend beleidsdocument. OZHZ vult het aan met beleid voor informatiebeveiliging op tactisch en operationeel niveau met specifieke (beleids-) documenten.

Het informatiebeveiligingsbeleid geldt voor alle activiteiten van OZHZ. Ook voor de activiteiten die vallen onder de Wpg geldt dat passende technische en organisatorische maatregelen moeten zijn genomen en geïmplementeerd, op basis van een risicoanalyse waaruit het risiconiveau blijkt met betrekking tot ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging. Deze maatregelen moeten bovendien periodiek worden geëvalueerd en zo nodig geactualiseerd.

Het volgende is dan van belang:
- OZHZ verwerkt in principe geen politiegegevens in de eigen systemen. Alleen het BRS bevat politiegegevens van de boa's van OZHZ. Met de externe verwerker, NatuurNetwerk B.V., is een verwerkersovereenkomst afgesloten op basis van het landelijk geldende model.
- In de Wpg zijn verplichtingen opgenomen met betrekking tot het uitvoeren van interne en externe audits. OZHZ moet als verwerkingsverantwoordelijke jaarlijks een interne audit uitvoeren en om de vier jaar een externe audit. De eerste externe audit vond in 2021 plaats. Voor de gebruikersorganisaties van het BRS is een Wpg-Assuranceverklaring beschikbaar. Hierin is opgenomen of/dat het systeem op aantoonbare wijze voorziet in de gestelde eisen voor informatiebeveiliging, onder andere het autorisatiebeleid, de logging, de artikelen 8, 9 en 13-informatielabeling, de cyberweerbaarheid, de rol van de bevoegd functionaris en de bewaartermijnen. Daarnaast is er een uitgebreide DPIA beschikbaar voor de gebruikers.
- De externe audit op het BRS maakt daarnaast onder andere duidelijk of/dat in BRS alleen politiegegevens kunnen worden verwerkt als dat nodig is voor de in de wet genoemde doeleinden, of/dat in BRS in beginsel geen gegevens kunnen worden verwerkt waarvoor geen doelbinding bestaat en of/dat gegevens in BRS niet op een met die doeleinden onverenigbare wijze kunnen worden verwerkt.
- Er is een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Dit houdt in dat OZHZ alleen die personen heeft geautoriseerd die vanuit hun functie en de wet toegang mogen hebben tot bepaalde politiegegevens voor alleen die gegevens. Er is een proces voor het toewijzen, wijzigen en intrekken van autorisaties ten behoeve van de toegang tot politiegegevens en er zijn maatregelen vastgesteld en geïmplementeerd met als doel dat periodiek de identiteit en de toegangsrechten van een gebruiker worden gecontroleerd. Daarmee borgt OZHZ de rechtmatige toegang tot de gegevens.

8. Functionaris Gegevensbescherming en privacyfunctionaris

<u>De Functionaris Gegevensbescherming (FG)</u>
Net als de AVG verplicht artikel 36 van de Wpg tot het aanstellen van de FG. Het is mogelijk dat meerdere organisaties samen één FG aanwijzen. De FG wordt door de verwerkingsverantwoordelijke tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van politiegegevens.

De FG is tenminste belast met de volgende taken:
- Het toezien op de naleving van de Wpg en op het beleid van OZHZ als verwerkingsverantwoordelijke, inclusief de toewijzing van autorisaties, bewustmaking en opleiding van de boa's en de audits, bedoeld in artikel 33 van de Wpg.
- Het informeren en adviseren van OZHZ als verwerkingsverantwoordelijke en de boa's over hun verplichtingen op grond van de Wpg en andere wetgeving over de bescherming van persoonsgegevens.
- Het geven van advies over DPIA's en het toezien op de uitvoering ervan.
- Het samenwerken met en optreden als contactpunt voor de AP.

- Het opstellen van een jaarverslag over zijn bevindingen.

De contactgegevens van de FG zijn openbaar en staan vermeld op de website van OZHZ. De FG is aangemeld bij de AP.

De samenwerkende organisaties in de Drechtsteden, waaronder ook OZHZ, hebben samen een FG aangewezen in het kader van de AVG. Blijkens haar website gaat de AP ervan uit dat deze dan ook toeziet op verwerkingen waarvoor de Wpg geldt. Vanwege het verschil in taakopdracht van de FG onder de AVG en die onder de Wpg, en vanwege het gebruik van het BRS (dat door geen enkele organisatie in de Drechtsteden wordt gebruikt), vindt OZHZ het wenselijk een aparte FG te benoemen in het kader van de Wpg. Het is mogelijk om dat samen met andere organisaties (bijvoorbeeld met de Drechtsteden of met de 4 andere omgevingsdiensten in Zuid-Holland) te doen of een extern bureau te vragen deze rol in te vullen. OZHZ geeft hieraan in 2021 /2022 invulling.

De privacyfunctionaris
Een organisatie met boa's hoeft naast de FG niet ook een privacyfunctionaris aan te wijzen als bedoeld in artikel 34 van de Wpg. Idee daarachter is dat veel organisaties met boa's daarvoor vaak te klein zijn. Het zou een onevenredige belasting geven. In de AVG is een privacyfunctionaris wel verplicht.

Normaliter geeft de privacyfunctionaris de verwerkingsverantwoordelijke en de personen die voor de verwerkingsverantwoordelijke werkzaam zijn advies over privacyvraagstukken en ziet toe op de rechtmatige verwerking van politiegegevens. De privacyfunctionaris houdt ook een overzicht bij van de schriftelijke vastlegging van de gegevens, als bedoeld in artikel 32, eerste lid, van de Wpg. Dat gaat over de doelen van de onderzoeken, bedoeld in artikel 9, tweede lid, van de Wpg, de verstrekking of doorgifte van politiegegevens, de feitelijke of juridische redenen die ten grondslag liggen aan een afwijzing, bedoeld in artikel 27, eerste lid, van de Wpg en een inbreuk op de beveiliging van persoonsgegevens, inclusief de feiten omtrent de inbreuk, de gevolgen ervan en de maatregelen die zijn getroffen ter correctie. De privacyfunctionaris stelt ook jaarlijks een verslag op van zijn bevindingen.

Binnen OZHZ, als boa-organisatie, zou dit betekenen dat de FG dit takenpakket van de privacyfunctionaris erbij zou moeten nemen. Dit is niet wenselijk. OZHZ heeft er daarom voor gekozen dat de beschreven taken van privacyfunctionaris worden uitgevoerd in goede samenwerking tussen de AVG-privacycoördinator, de coördinator van de boa's en de Wpg-FG.

9. Rechten van betrokkenen

De rechten van betrokkenen onder de AVG staan uitgebreid beschreven in het privacybeleid van OZHZ. Op hoofdlijnen zijn deze rechten op grond van de Wpg gelijkluidend.

Specifiek voor de Wpg geldt nog het volgende:
- De verwerkingsverantwoordelijke biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit beknopt, toegankelijk en duidelijk, zodat de betrokkene zijn rechten kan uitoefenen. De informatievoorziening voldoet aan de eisen uit artikel 24b van de Wpg.
- Bij uitstel, beperking of achterwege laten van de verstrekking van informatie bedoeld in 24b van de Wpg is het uitstel, de beperking of het achterwege laten alsmede de duur van deze maatregel onderbouwd.
- Een verzoek om inzage, rectificatie of vernietiging wordt afgewezen voor zover dit noodzakelijk en evenredig is ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures, ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, ter bescherming van de openbare veiligheid, ter bescherming van de rechten en vrijheden van derden, ter bescherming van de nationale veiligheid en ingeval van een kennelijk ongegrond of buitensporig verzoek. Een gehele of gedeeltelijke afwijzing van een verzoek is schriftelijk en bevat de redenen voor de afwijzing.

OZHZ geeft hieraan uitvoering door op de eigen website en op de website van de externe verwerker van het BRS (NatuurNetwerk B.V.) te melden wat de rechten van betrokkenen zijn en hoe men daarvan gebruik kan maken. De verwerkte politiegegevens, met uitzondering van de gegevens over de boa's, vallen onder de uitsluitingsgronden van de Wpg. De externe verwerker NatuurNetwerk B.V. informeert OZHZ over een ingekomen verzoek, opdat de boa de informatie ter inzage kan aanbieden, rectificeren of verwijderen.

10. Het bewaren van politiegegevens

De AVG schrijft voor dat gegevens niet langer bewaard mogen worden dan noodzakelijk voor het doel waar ze voor nodig zijn. Dit doel wordt beschreven in verschillende wetten, daarom lopen de bewaartermijnen van persoonsgegevens uiteen. Daar waar er geen wettelijke bepaling is die voorziet in een

verplichte bewaartermijn, heeft OZHZ een eigen besluit genomen over de bewaartermijn. Daarnaast geldt de Archiefwet voor het bewaren van papieren en elektronische documenten. De bewaartermijnen staan vermeld in het register van verwerkingen.

Politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. OZHZ dient als verwerkingsverantwoordelijke te voorzien in voldoende waarborgen om te bewerkstelligen dat de gegevens conform de wet worden gecontroleerd, verwijderd en vernietigd. Politiegegevens dienen na verwijdering nog maximaal vijf jaar worden bewaard. Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen als genoemd in de Archiefwet voldaan.

Binnen het BRS worden alle politiegegevens gelabeld in artikel 8, 9 en 13 informatie. Voor elk label is de bewaartermijn conform de wettelijke bepaling geconfigureerd, zodat geborgd wordt dat deze politiegegevens niet langer worden bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt.

11. Het ter beschikking stellen en verstrekken van politiegegevens

De Wpg maakt een onderscheid tussen het ter beschikking stellen van politiegegevens en het verstrekken ervan. Het ter beschikking stellen van politiegegevens houdt in dat deze in principe worden gedeeld met eenieder die de gegevens nodig heeft voor de uitoefening van zijn taak. Bij dit ‘need to know’-principe dient altijd een noodzakelijkheids-, proportionaliteits- en subsidiariteitsafweging te worden gemaakt. Het ter beschikking stellen voltrekt zich dus binnen het Wpg-domein.

Bij het verstrekken van politiegegevens gaat het om het delen van gegevens buiten het Wpg-domein. In dat geval moet zijn geborgd dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wpg en het Bpg zijn genoemd. Geborgd moet ook zijn dat wanneer gegevens verstrekt worden, er wordt voldaan aan de documentatieplicht en dat de verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag indien dit vereist is in de wet. Het gaat dan bijvoorbeeld om verstrekkingen aan de burgemeester, een toezichthouder, een advocaat of een functionaris in het kader van de Wet bibob. Uitgangspunt is overigens dat OZHZ geen politiegegevens verstrekt aan anderen dan medewerkers van politie, Koninklijke marechaussee en/of het OM, voordat er vooraf met de boacoördinator is getoetst of deze verstrekking voldoet aan de wetgeving. OZHZ verstrekt geen politiegegevens aan ontvangers in derde landen of internationale organisaties.

OZHZ dient ook inzicht te hebben in de samenwerkingsverbanden waarbij politiegegevens worden verstrekt. In de beslissing voor het verstrekken van politiegegevens ten behoeve van een samenwerkingsverband wordt vastgelegd:
- Ten behoeve van welk zwaarwegend algemeen belang de verstrekking noodzakelijk is.
- Ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt.
- Het doel waartoe dit is opgericht.
- Welke gegevens worden verstrekt.
- De voorwaarden onder welke de gegevens worden verstrekt, en
- Aan welke personen of instanties de gegevens worden verstrekt.

De daadwerkelijke verstrekking van gegevens dient ook te worden vastgelegd.

Vooralsnog zijn er vanuit OZHZ geen samenwerkingsverbanden waarbij politiegegevens worden verstrekt. Mocht dit wel het geval zijn dan zal OZHZ jaarlijks de samenwerkingsverbanden waarbij politiegegevens worden verstrekt in kaart brengen.

Het BRS voorziet in een functionaliteit waarmee verstrekkingen kunnen worden geregistreerd en gedocumenteerd. Daarnaast kan OZHZ gebruik maken van de Verstrekkingenwijzer voor boa's en is binnen OZHZ een van de boa's aangewezen als coördinator bij het doen van verstrekkingen.
Tot slot beschikt het BRS over functionaliteiten om gegevens op een veilige manier, door middel van tweefactor authenticatie en beveiligde verbinding, te verstrekken aan personen.

12. Het melden van datalekken

Artikel 33a van de Wpg bepaalt dat een datalek ('inbreuk op de beveiliging') onverwijld en uiterlijk binnen 72 uur nadat ervan kennis is genomen moet worden gemeld aan de AP, tenzij het niet waarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van personen met zich meebrengt. Als de melding na 72 uur wordt gedaan, gaat deze vergezeld van een motivering voor de vertraging.

OZHZ moet het datalek ook aan de betrokkenen mededelen als deze inbreuk waarschijnlijk een hoog risico voor de rechten en vrijheden van personen met zich meebrengt.

Op deze mededelingsplicht zijn enkele uitzonderingen van toepassing, onder andere als de mededeling achterwege moet blijven ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures en ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

Indien sprake is van een datalek bij een externe verwerker gelden dezelfde regels. In de verwerkersovereenkomst met NatuurNetwerk B.V. zijn hierover nadere afspraken vastgelegd vanwege het gebruik van het BRS.

13. Bewustwording binnen OZHZ

Het zorgvuldig omgaan met persoonsgegevens is enerzijds een kwestie van het organiseren van een goede informatieveiligheid en het zorgvuldig inrichten van werkprocessen, anderzijds is het een zaak van bewustwording bij de boa's van OZHZ. Het bewustzijn wordt voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.

De boa's van OZHZ verwerken de politiegegevens in principe alleen in het BRS. Dit betreft de processenverbaal en de bestuurlijke strafbeschikkingen op het gebied van de groen en grijze (milieu e.a.) wet- en regelgeving. Daartoe volgen zij regelmatig trainingen en opleidingen en gelden interne werkinstructies en afspraken. De speciaal ontwikkelde interactieve e-learning van het BRS laat nieuwe gebruikers in eigen tijd en tempo kennis maken met het systeem en maakt ongelimiteerd oefenen mogelijk. Daarnaast maakt OZHZ gebruik van de aangeboden online seminars en cursussen gericht op het genereren van managementinformatie, het gebruik van de CJIB-transactiemodule of verdere uitleg van een andere specifieke functionaliteit in het systeem.

De externe audit op het BRS dient de werking aan te tonen dat, alvorens boa's gebruik mogen maken van het BRS, zij een training moeten volgen en praktijkopdrachten met goed gevolg moeten hebben afgerond.

14. Open communicatie

Betrokkenen moeten erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. OZHZ creëert dat vertrouwen door inzichtelijk te maken, door middel van verschillende communicatiekanalen, op welke wijze hij persoonsgegevens verwerkt en beheert. Dit staat in de privacyverklaring van OZHZ die op de website is te vinden: www.ozhz.nl/privacy. Ook het register van verwerkingen en informatie over de rechten van betrokkenen zijn daar te vinden.

Aldus vastgesteld door het dagelijks bestuur van de Omgevingsdienst Zuid-Holland Zuid op 11 november 2021.