



Gegevensbeschermingseffectenbeoordeling Wpg

**OBI4wan
Social Media
webcaretooling**

Gegevensbeschermingseffectenbeoordeling Wet Politiegegevens

Versie definitief 1.0

Versie datum 2 december 2022

Rubricering Politie Intern

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	10-10-22	Concept 0.1 opgesteld.	
0.2	11-10-2022	Concept 0.1 aangepast op basis van review HK.	
0.3	17-10-2022	Concept 0.2 aangepast en aangevuld op basis van afstemming met HK en gebruikersinstructie OBi4wan.	
0.4	01-11-2022	Concept 0.3 aangevuld n.a.v. de 'gebruikersinstructie' en finetuning.	
0.5	03-11-2022	Laatste concept, aangepast op basis van laatste informatie.	
1.0	02-12-2022	Aanvullend risico Facebookpagina's toegevoegd en definitieve versie 1.0 gemaakt.	

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie

Review commentaar

Versie	Wanneer	Wie	Functie

Basisinformatie

Basisinformatie met betrekking tot deze verwerking van persoonsgegevens

Datum:	10-10-2022
Naam van de verwerking:	OBI4wan
Ingangsdatum van de verwerking:	Er wordt al 5 jaar gewerkt met OBI4wan, maar geen GEB daarop uitgevoerd. Er vindt nu een productgerichte uitvraag via Inkoop plaats voor de verlenging van het contract met OBI4wan voor de applicatie OBI Engage. Begin 2023 moet deze verlenging zijn geformaliseerd, daarom nu een GEB uitvoeren.
Politieonderdeel verantwoordelijk voor de verwerking;	Dienstverlening
Organisatie/Afdeling/Portefeuillehouder waar de verwerking plaatsvindt:	Janny Knol, portefeuillehouder Dienstverlening
Contactpersoon m.b.t. deze verwerking:	5.1.2.e , landelijk Social Media Regisseur
Privacyfunctionaris:	Oost-Nederland, 5.1.2.e
Betrokken bij deze GEB:	GEB-Regie, privacy-adviseur 5.1.2.e

Functionaris gegevensbescherming	5.1.2.e
Datum:	<invullen>
Reactie: <invullen>	

Gezien door verwerkingsverantwoordelijke

Naam:	Janny Knol
Functie:	Portefeuillehouder Dienstverlening
Datum:	<invullen>
Opmerkingen: <invullen>	

Inhoudsopgave

Documentinformatie	2
Basisinformatie.....	3
Inhoudsopgave.....	3
1. Managementsamenvatting	6
1.1. Inleiding	6
1.2. Doelstelling	6
1.3. Aanpak	6
1.4. Bevindingen en maatregelen	6
1.5. Vervolgproces.....	6
A. Beschrijving kenmerken gegevensverwerking	7
1. Voorstel.....	7
1a. Voorstel van de verwerking.....	7
1b. Geef aan waarom sprake is van een hoog risicoverwerking waarvoor volgens de Wpg een GEB moet worden opgesteld.	8
2. Politiegegevens.....	8
3. Gegevensverwerking	10
Benoem de datastroom in onderstaande kolom.....	10
4. Doel van de verwerking.....	10
5. Betrokken partijen	11
6. Belangen bij de gegevensverwerking.....	12
7. Verwerkingslocaties	12
8. Technieken en methoden.....	Fout! Bladwijzer niet gedefinieerd.
8a. Technieken en methoden van de gegevensverwerking	13
8b. Big data.....	14
9. Juridisch en beleidsmatig kader	15
10. Verwerkingstermijnen.....	16
B. Beoordeling rechtmatigheid gegevensverwerking	16
11. Doeleinden / wettelijke grondslag.	16
12. Bijzondere politiegegevens	17
13. artikel 13 ondersteunende taken	18
14. Noodzaak en evenredigheid	18
15. Rechten van betrokkenen	19
C. Beschrijving en beoordeling risico's voor de betrokkenen	20
16. Risico's voor de betrokkenen	20
De privacy risico analyse Wpg	20
Risicomatrix verwerkingen Wpg	21
Risico analyse privacy issues Wpg verwerkingen.....	22
D. Maatregelen en restrisico's	24
<i>In onderdeel D wordt geadviseerd welke maatregelen getroffen kunnen worden om de geconstateerde risico's uit onderdeel C naar een aanvaardbaar niveau te brengen. Risico's volledig reduceren is (vaak) niet mogelijk. Dit betekent dat er altijd een resterend risico zal overblijven. De verwerkingsverantwoordelijke dient te beschrijven hoe het tot dit restrisico is gekomen en waarom deze aanvaardbaar wordt geacht.</i>	
17. Maatregelen	24
Een passend beveiligingsniveau veronderstelt dat gewerkt wordt met een planning- en controlcyclus (plan-do-check-act) aan de hand waarvan kan worden beoordeeld of de beveiliging steeds adequaat is voor de huidige stand van de techniek en de organisatie.....	24
Voor te treffen maatregelen kan worden aangehaakt bij beveiligingskaders en -standaarden, beste praktijken en goedgekeurde gedragscodes en certificeringsmechanismes. Wanneer een of meerdere van toepassing zijn op de	

gegevensverwerkingen, beschrijf dan specifiek welke beveiligingsstandaarden, praktijken, gedragscodes en/of certificeringsmechanismes van toepassing zijn en op welke manier deze in de praktijk van toepassing zijn op de gegevensverwerkingen. Bij het bepalen van de gepaste maatregelen moet ook rekening gehouden worden met maatregelen die voortvloeien uit de Baseline Informatiebeveiliging Overheid (BIO).24

1. Managementsamenvatting

1.1. Inleiding

Voor je ligt een gegevensbeschermingseffectbeoordeling (hierna: GEB), uitgevoerd op grond van de Wet Politiegegevens (hierna: Wpg). Een GEB wordt uitgevoerd in het geval dat een gegevensverwerking waarschijnlijk een wettelijk hoog privacy-risico oplevert voor de personen van wie een organisatie gegevens verwerkt.

1.2. Doelstelling

Het doel van deze GEB is om op een heldere en structurele manier inzicht te verkrijgen in de risico's die gepaard gaan met de verwerking van politiegegevens. Vervolgens worden er in deze GEB aanbevelingen gedaan om de geconstateerde risico's te kunnen reduceren tot een acceptabel niveau.

1.3. Aanpak

Deze GEB Wpg is gebaseerd op het Rijksmodel. Deze GEB is ingevuld door 5.1.2.e, landelijk Social Media Regisseur in samenspraak met betrokken privacy adviseur van GEB R. In onderdelen A en B zijn kenmerken van de gegevensverwerking en de rechtmatigheid onderzocht. Hieruit zijn vervolgens privacy risico's geformuleerd. De privacy risicoanalyse is terug te vinden in de onderdelen C en D van het GEB formulier. De analyses voor informatiebeveiliging zijn beschikbaar bij het IB-kwartier.

1.4. Bevindingen en maatregelen

In 2019 is een IB-analyse uitgevoerd voor OBI Engage. Van de aanbevelingen om risico's te mitigeren zijn er een aantal uitgevoerd en enkele zijn in uitvoering. De maatregelen van de verwerking dienen te worden opgepakt door de verwerkingsverantwoordelijke zelf. De maatregelen voor de ondersteunende systemen worden reeds opgepakt. Meer gedetailleerde informatie over deze aanbevelingen zijn te vinden in onderdeel D van deze GEB.

Uitgevoerd zijn:

- weghalen van de autorisatie bij de superuser om een nieuwe gebruiker aan te maken voor OBI. Deze zit alleen nog op het niveau van een Eenheidsbeheerder en Toplevelbeheerder.
- De aanbeveling om alle nieuwe aanvragen voor een OBI inlog te laten registreren via de ATL is in gang gezet. Zal in Nov 2022 gerealiseerd zijn.
- 2FA is beschikbaar in 2023. Opgenomen in Roadmap van 2023 OBI. Benodigde budget binnen de politie aangevraagd. Met leverancier OBI4wan is er overleg om dit onderdeel in Q1 van 2023 uit te voeren.
- Aanbeveling voor de trainingen: trainingsomgeving voor OBI Engage is aangekocht en is 1-1-2023 operationeel om politiemedewerkers te trainen in het werken met OBI Engage.

Aanvullend risico

- Op 3 december 2022 is in de definitieve versie 0.5 onderstaand risico toegevoegd en die versie afgerond als definitieve versie 1.0
-

De maatregelen dienen door de Product owner ingevoerd te worden in het daarvoor beschikbare systeem Jira en de voortgang via dit systeem ook gemonitord.



GEB registreren in
JIRA.docx

1.5. Vervolproces

Met de definitieve versie GEB wordt de CIO aanvraag gedaan voor de Cloudmigratie en kan de productgerichte aanvraag via Inkoop in gang worden gezet.

Begin 2023 moet de verlenging van het contract met OBI4wan voor de applicatie OBI Engage afgerond zijn.

A. Beschrijving kenmerken gegevensverwerking

Onder A wordt de eerste stap beschreven van de GEB: een overzicht van alle relevante feiten van de (voorgenomen) gegevensverwerking. Essentieel is dat de feiten helder en volledig zijn, want het resterende deel van de GEB is gebaseerd op wat in dit onderdeel is beschreven.

Beschrijf op gestructureerde wijze de (voorgenomen) gegevensverwerking, de verwerkingsdoeleinden en de belangen bij de gegevensverwerking.

1. Voorstel

1a. Voorstel van de verwerking

Beschrijf het voorstel waar de GEB op toeziet op hoofdlijnen en benoem hoe het voorstel tot stand is gekomen en wat de beweegredenen zijn achter de totstandkoming van het voorstel.

Antwoord:

Inleiding

OBI4wan is een applicatie waarmee grootschalig meldingen, klachten, tips e.d. wordt verwerkt, die burgers zelf actief via hun eigen Social Media accounts naar de Social Media accounts van de Politie sturen Twitter, Facebook of Instagram.

De Politie beschikt over ruim 2000 Social Media accounts bij de eenheden, wijkteams e.d.

Door middel van OBI4wan kan de Politie op een laagdrempelige en door burgers inmiddels veel gebruikte manier met de burgers communiceren in het kader van de dagelijkse Politietaken.

De gegevens binnen OBI4wan-Engage zijn afkomstig van online klantcontacten. Denk daarbij aan tweets van Twitter, Facebookberichten, Instagramberichten gericht aan een basisteam, regionale eenheid, wijkagenten of de landelijke eenheid.

Het gaat om privéberichten of om openbare berichten (nieuws e.d.) die via privéberichten door burgers naar de sociale media accounts van Twitter, Facebook en Instagram van de Politie worden gestuurd.

Binnen een Eenheid wordt er tussen RSC's, Basisteam, communicatieteam en andere afdelingen op het gebied van online klantcontact samengewerkt. Elk team handelt haar eigen berichten af (WBT of App), of werkt samen met andere teams, eenheden of afdelingen. Dat gaat zowel binnen OBI4wan-Engage (overzetten of toekennen van berichten), als buiten OBI4wan-Engage door berichten te mailen naar afdelingen zoals DRIO/OPS/Meldkamer.

De diverse soorten berichten met informatie en persoonsgegevens van burgers, die zij sturen naar de Politie zijn voor de Politie politiegegevens op grond van de artikel 1 onder a Wpg, artikel 3 Wpg en artikel 8 Wpg.

OBI Engage

Het bedrijf OBI4Wan levert het product OBI Engage. Dit product heeft verschillende modules.

De politie maakt gebruik van de Webcare modules om de vele Social Media accounts van de politie te volgen op binnengekomen berichten en deze te verwerken voor verdere afhandeling.

De binnengekomen berichten van burgers worden door middel van een algoritme gescand op bepaalde woorden, zogenaamde sentimenten. Op basis van deze sentimenten worden de berichten gekenmerkt met een grijze, oranje of groene kleur. Op basis van deze kleuren-categorisering wordt de behandelend politiemedewerker geïnformeerd voor een effectieve en efficiënte afhandeling/beantwoording en alertheid voor de beantwoording van bepaalde berichten met een negatief sentiment.

- groen, neutraal/niets bijzonders,
- grijs, mogelijkheid van negatieve sentimenten
- oranje, negatieve sentimenten

De Politie beschikt over de database met woorden op basis waarvan de binnengekomen berichten worden gecategoriseerd.

1b. Geef aan waarom sprake is van een hoog risicoverwerking waarvoor volgens de Wpg een GEB moet worden opgesteld.

Antwoord:

De verwerking van data in OBI Engage wordt beschouwd als een 'hoog risico' verwerking, omdat:

Ten eerste OBI4wan is een applicatie waarmee grootschalig berichten van burgers worden verwerkt met een diversiteit aan informatie aan de politie.

Het gaat om berichten betreffende een melding, klacht, tips, informatie over derden e.d., die burgers zelf actief naar de Politie sturen. Het kunnen dus ook berichten zijn met gevoelige informatie of bijzondere persoonsgegevens.

Ten tweede categoriseert de tool OBI Engage de binnengekomen berichten, met gebruik van een algoritme met een database met woorden, naar de mate van 'sentiment'. Door het toekennen van een sentiment, aangeduid met een kleur aan het bericht, kan de afhandeling efficiënter en effectiever plaatsvinden door politiemedewerkers.

Ten derde vindt de verwerking van de data plaats in een 'public cloud' van de leverancier.

2. Politiegegevens

Beschrijf alle politiegegevens die worden verwerkt. Classificeer deze gegevens naar: algemeen en bijzonder (en bij bijzonder de categorie van bijzondere politiegegevens die wordt/worden verwerkt). Geef per categorie betrokkenen aan welke (categorieën) politiegegevens worden verzameld.

Categorie betrokkenen	Politiegegevens	Type politiegegevens Algemene politiegegevens of bijzondere politiegegevens (de categorie van bijzondere politiegegevens)	Bron
Burgers	Accountgegevens van burgers van hun Twitter-, Facebook-, of Instagram-account.	Algemeen	Social Media account van de betrokken burger die een bericht stuur naar een Social Media account van de Politie.
	a) Naam -, adres - en woonplaatsgegevens	Algemeen	idem
	b) Telefoonnummers	Algemeen	Idem
	c) Emailadressen of andere adressen voor elektronische communicatie.	Algemeen	Idem
	d) procesverbaalnummer (komt incidenteel voor)	Algemeen	Idem
	e) Geslacht, geboortedatum en/of leeftijd	Algemeen	Idem
	f) pasfoto / avatar	Algemeen	Idem

Aanvullende informatie over de politiegegevens:

Categorie van betrokkenen	Soort persoonsgegevens	Bijzondere persoonsgegevens (ja/nee)	Hoe worden de persoonsgegevens verkregen?	Doel waarvoor de gegevens worden verwerkt	Bewaartermijn van de gegevens
Burgers	Persoonsgegevens die door burgers zelf zijn ingevuld en dus te zien zijn op de eigen social media accounts. Extra : contactgegevens die door de politie aan de burger gevraagd wordt die noodzakelijk zijn voor daadwerkelijke uitvoering van dienstverlening (webcare)	Bijzondere persoonsgegevens die door de burger zelf zijn vermeld in het bericht aan de politie en/of beeldmateriaal dat herleidbaar is naar natuurlijke personen zoals bijvoorbeeld een profielfoto of een avatar.	Accounts social media platforms van burgers.	Deze gegevens zijn noodzakelijk om via webcare een betere, adequate en kwalitatieve dienst te kunnen verlenen in de vorm van het beantwoorden van berichten of op basis van een bericht tot uitvoering over te gaan.	30 maanden

Categorieën van ontvangers	Welke categorie van gegevens (zoals vermeld bij vraag 7)	Intern of extern politie	Doel toegang tot gegevens
Politie, Medewerkers webcaretool	Algemene persoonsgegevens die door burgers zelf zijn ingevuld en dus te zien zijn op de eigen social media accounts. Bijzondere persoonsgegevens die door een burger in een bericht worden vermeld. Extra: contactgegevens die door de politie aan de burger gevraagd wordt, die noodzakelijk zijn voor daadwerkelijke uitvoering van dienstverlening (webcare)	Extern (SAAS applicatie)	Deze informatie is nodig om in te kunnen loggen in de webcaretool en bij te kunnen sturen waar nodig. Deze gegevens zijn noodzakelijk om via webcare een betere, adequate en kwalitatieve dienst te kunnen verlenen.
Politie	Politie emailadres	Intern en extern	Herleidbaar uit accountinformatie van de betreffende medewerkers
Webcaretool beheer	Persoonsgegevens die door burgers zelf zijn ingevuld en dus te zien zijn op de eigen social media accounts. Extra: contactgegevens die door de politie aan de burger gevraagd wordt die noodzakelijk zijn voor daadwerkelijke uitvoering van dienstverlening (webcare)	Extern (SAAS applicatie)	Technische beheer webcaretool

3. Gegevensverwerking

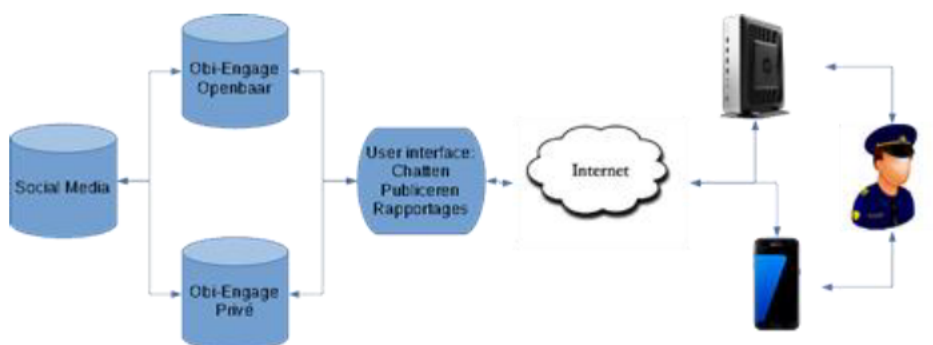
Geef de voorgenoemde gegevensverwerking weer en geef aan welke politiegegevens worden verwerkt per voorgenoemde gegevensverwerking. Per GEB is er sprake van 1 hoofdverwerking en verschillende sub-verwerkingen. Beschrijf deze verwerkingen en benoem hierbij ook de daarbij horende Bedrijfsreferentiemodel (hierna: BRM) verwerkingsprocessen. Beschrijf de datastroom in de kolom. Wanneer er reeds een gegevensstroomschema of werkprocesbeschrijving is mag deze toegevoegd worden als bijlage. Voeg aanvullende informatie toe in het tekstveld.

Benoem de datastroom in onderstaande kolom

Input	Throughput	Output
Meldingen, vragen, tips, klachten of andere (gevoelige) informatie van burgers via hun eigen Social Media accounts Facebook, Twitter of Instagram, die actief gedeeld worden via de betreffende Social Media accounts van de Politie.	Berichten komen binnen in de Social Media accounts van de Politie op de cloud-servers van OBI4wan. Via userinterface kan de politiemedewerker de beantwoording of verdere afhandeling verzorgen.	Antwoorden op de Social Media berichten van burgers. Incidenteel een directie spoedactie via de Meldkamer.

Aanvullende informatie over de gegevensverwerking:

Procesplaat gegevensverwerking



4. Doel van de verwerking

Beschrijf het doel van de voorgenoemde gegevensverwerking. Voeg aanvullende informatie toe in het tekstveld.

Gegevensverwerking	Het doel van de verwerking
Meldingen, tips, klachten en informatie van betrokkenen aan de Politie via de webcaretool OBI4wan (berichten met algemene en/of bijzondere persoonsgegevens of andere algemene of gevoelige informatie).	Doel: betere dienstverlening aan de burger door de mogelijkheid van een directe vorm van communicatie via de Social Media kanalen van burgers (betrokkenen) naar de Politie. Er worden alleen persoonsgegevens verwerkt / gebruikt welke noodzakelijk zijn om op een adequate en efficiënte manier dienstverlening via OBI4wan te bewerkstelligen. De Politie verwerkt de persoonsgegevens om: antwoord te kunnen geven op vragen, klachten enz. (zowel privé als openbare berichten) die mensen stellen aan de bij de politie in gebruik zijnde social media kanalen.

	Misbruik of valse meldingen worden vastgelegd bij gebruikersdetails om verder misbruik te worden voorkomen.

Aanvullende informatie over de verwerkingsdoeleinden:

'Met de zakelijke Social Media accounts van de Politie wordt bijgedragen aan de volgende doelstellingen: Betere en laagdrempelige communicatie met de burger en betere politiestatistiek door snelle en directe beantwoording.

Op een structurele manier bijdragen aan politiewerk; met professionele ruimte.

Hierdoor beoogd effect van meer legitimiteit, meer vertrouwen in de politie.

Socialmedia-accounts zijn makkelijk vindbaar, herkenbaar en benaderbaar.

Functioneren als één korps. Zelfde niveau van dienstverlening voor elke burger, social media is voorspelbaar en interactief voor elke burger'.

<citaat uit Beleidsdocument: Online op één lijn Communiceren via social media>

5. Betrokken partijen

Benoem alle organisaties die betrokken zijn per voorgenomen gegevensverwerking. Deel deze organisaties in onder de rollen: verwerker, sub-verwerker, verstrekker, Wpg en niet Wpg ontvanger en derde. Benoem ook welke functies/afdelingen binnen deze organisaties politiegegevens verstrekt krijgen, ter beschikking gesteld krijgen of toegang krijgen tot persoonsgegevens. Voeg aanvullende informatie toe in het tekstveld.

Naam partij	Rol partij	Juridische grondslag	Type politiegegevens
Verstrekker Burgers	Verstrekt informatie en persoonsgegevens via de berichten die via Twitter, Facebook of Instagram via de Social Media accounts van de Politie worden gestuurd.	Avg, artikel 4.1.	
Verwerkings- verantwoordelijke Politiemedewerkers webcaretool RSG's, Meldkamer.	Beantwoorden van vragen in de Social Media berichten van burgers en incidenteel het direct doorzetten naar de Meldkamer bij spoedzaken.	Artikel 8 Wpg dagelijkse politietaken.	Artikel 1 onder a en b Wpg en artikel 5 Wpg, algemene en bijzondere persoonsgegevens
Verwerkings- verantwoordelijke Functioneel beheer Politie.	Functioneel- en technisch beheer webcaretool OBI Engage, waaronder zorgdragen voor autorisatiebeheer (wie heeft toegang tot de applicatie), inrichten van de applicatie op basis van de eisen IB en Privacy, afstemming met de leverancier bij technische maatregelen, zorgdragen voor opleiding en training.	Artikel 6a Wpg (toegang tot politiegegevens).	Artikel 1 onder a en b Wpg en artikel 5 Wpg, algemene en bijzondere persoonsgegevens. Persoonsgegevens van politiemedewerkers die toegang hebben tot de applicatie: voor- en achternaam en emailadres.
Verwerker: OBI4wan b.v.,	OBI4wan is verwerker. Verwerkersovereenkomst  Verwerkersovereenkomst politie 5.1.2.e	Artikel 6c Wpg (Verwerker).	Artikel 6a Wpg (toegang tot politiegegevens). Artikel 1 onder a en b Wpg en artikel 5 Wpg, algemene en bijzondere persoonsgegevens.

	Verwerkersovereenkomst is nog niet afgesloten/ondertekend !!! Deze wordt ondertekend nadat de uitvraag is gedaan. Wordt door afdeling Inkoop geregeld na de gunning.		Persoonsgegevens van politiemedewerkers die toegang hebben tot de applicatie: voor- en achternaam en emailadres.
--	--	--	--

Aanvullende informatie over de betrokken partijen:

--

6. Belangen bij de gegevensverwerking

Beschrijf alle belangen die de betrokken partijen hebben bij de voorgenomen gegevensverwerking. Voeg aanvullende informatie toe in het tekstveld.

Betrokken Partij	Belangen
Politie	Efficiënte en effectieve communicatiekanalen beschikbaar stellen voor burgers gericht op Social Media mogelijkheden voor laagdrempelige communicatie.
Burgers	Laagdrempelige mogelijkheid voor communicatie met de Politie die aansluit bij de Sociale Media kanalen van burgers.
OBI4wan	Leverancier van de SaaS-voorziening OBI4wan en verwerker via cloudhosting van de applicatie.

Aanvullende informatie over de belangen:

--

7. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerking plaatsvinden. Beschrijf de grondslag van de doorgifte (bv. adequaatheidsbesluit) dat van toepassing is wanneer verwerkingslocaties buiten de Europese Economische Ruimte (EER) bevinden. Voeg aanvullende informatie toe in het tekstveld.

Gegevensverwerking	Verwerkingslocaties	Doorgifte grondslag	Passende waarborgen
Berichtenverkeer via OBI Engage	Nederland en binnen de EER	n.v.t.	Zie voor details hoofdstuk 17 mitigerende maatregelen. Verwerkersovereenkomst wordt afgesloten met de leverancier.

Aanvullende informatie over de verwerkingslocaties:

--

8a. Technieken en methoden van de gegevensverwerking

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de politiegegevens worden verwerkt. Benoem of sprake is van bijvoorbeeld (semi-) geautomatiseerde besluitvorming, profilering, een cloudoplossing of big dataverwerkingen (kwaliteitskader Big data) en, zo ja, beschrijf waaruit dat bestaat.

Beschrijving van de technieken en methoden van de gegevensverwerking:

Toelichting

Webcare middel de applicatie OBI Engage van OBI4wan is de structurele, real-time serviceverlening van de politie via sociale media (Facebook, Twitter en Instagram) aan burgers.

Met Webcare antwoordt de politie op vragen, verstrekt ze informatie en lost ze klachten op. Dat doet de politie zowel reactief als op eigen initiatief.

Logging

(Audit) logging is aanwezig op de applicatie OBI Engage.

Authenticatie en Autorisatie volgens het autorisatie beleid NP.

Gebruikersnaam + wachtwoord + 2FA voor authenticatie, wordt geïmplementeerd in de eerste helft van 2023.

Autorisaties worden ingeregeld conform specificatie in ATL tool.

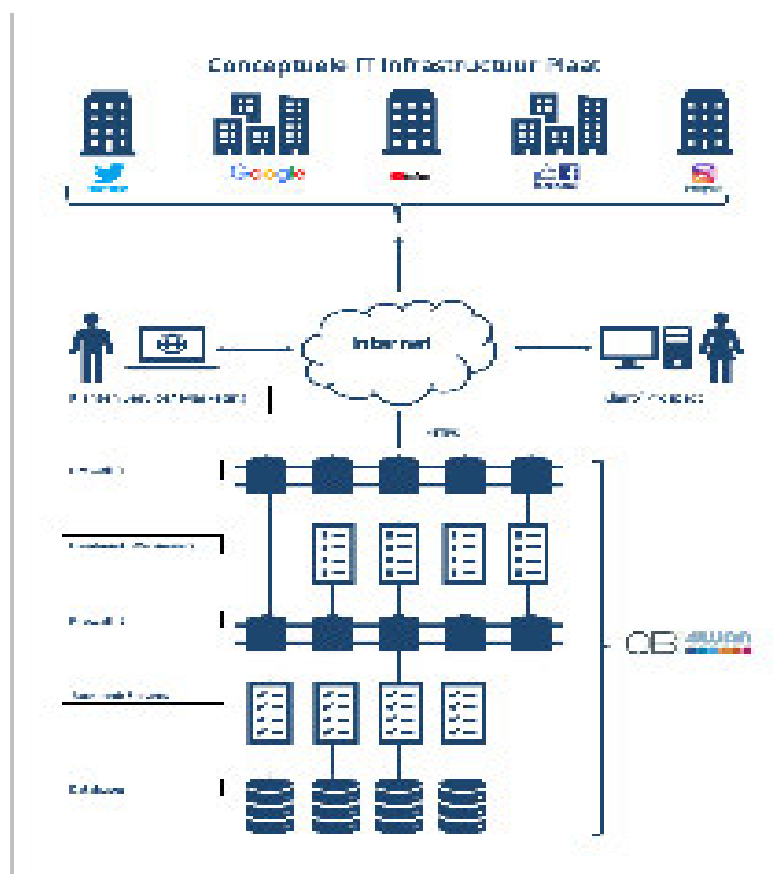
Autorisatie via machtigingen en rollen structuur.

Zie voor meer technische details onderstaande document.



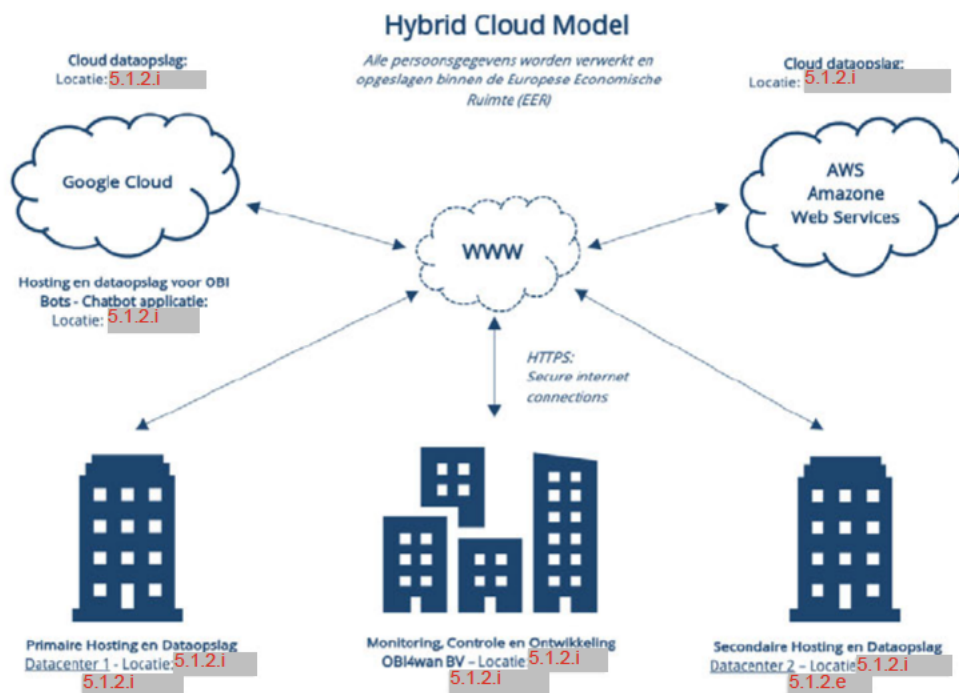
PHDPCSUP-OBIEng
age-290922-1240-10

Architectuurplaat



Infrastructuur

OBI Engage is een SAAS oplossing die gehost wordt in een datacenters op het grondgebied van de EER. Verschillende onderdelen worden gehost in verschillende datacenters. Zie onderstaande plaat:



De inhoudelijke informatie (data) van de gegevens van burgers wordt niet verwerkt op de servers van een externe cloudprovider of OBI4wan. De berichten zelf van de burgers met de inhoudelijke informatie wordt namelijk gehost op de servers van de Politie.

OBI4Wan is ISO27001 gecertificeerd.

8b. Big data

Beschrijf hieronder of u de verwerking van big data getoetst heeft aan het kwaliteitskader big data.

Beschrijving van de toetsing van de big data-verwerking aan het kwaliteitskader big data:

Er vindt geen big data verwerking van de informatie plaats.

De berichten worden gescand met de inzet van een algoritme op basis van een vooraf ingevulde woorden-database. Op basis van de, door de burger, geschreven specifieke woorden, bijvoorbeeld scheldwoorden worden de berichten gecategoriseerd met een kleur voor het betreffende sentiment van het bericht. Dit om de betreffende politiemedewerker er te attenderen dat een bericht met meer zorg behandeld moet worden.

Uiteindelijk is het de politiemedewerker die het bericht leest en beoordeelt en op basis van zijn/haar interpretatie het bericht beantwoord, ongeacht de kleuren-categorie en het vooraf aangegeven sentiment van het bericht.

9. Juridisch en beleidsmatig kader

Benoem alle wet- en regelgeving en beleid met mogelijke gevolgen voor de voorgenomen gegevensverwerking. De AVG en de Richtlijn¹ hoeven niet genoemd te worden. Voeg aanvullende informatie toe in het tekstveld.

Gegevensverwerking	Juridisch en/of beleidsmatig kader	Wetsartikelen
Door burgers via hun eigen Sociale Media account verstuurd berichten aan de Politie, met algemene persoonsgegevens, bijzondere persoonsgegevens en/of met algemene of gevoelige informatie.	Verwerking in het kader van de dagelijkse politietaak, artikel 8 Wpg. Berichten worden intern verder verwerkt voor beantwoording en afhandeling op grond van artikel 3 Wpg.	Artikel 8 Wpg, Artikel 3 Wpg.
	Beleid : Herijkt social media beleid 2020, zie voor het beleidsdocument hieronder in aanvullende informatie; Alle social media account moeten gekoppeld worden aan de webcaretool OBI4wan. Goedgekeurd door KMTD.	Beleidsdocument: Online op één lijn Communiseren via social media: zakelijk en privé, Directie Communicatie Status: Definitief Versie: Versie 1 Datum: september 2020
Inloggegevens van geautoriseerde politiemedewerker: voor- en achternaam en emailadres.	Autorisatiebeleid NP	Artikel 6a Wpg.
Verwerking middels een applicatie zoals Webcaretool OBI Engage	Beleidsdocument Online op één lijn.	Zie onderstaande toelichting op de inzet van een webcaretool.

Aanvullende informatie over het juridisch en beleidsmatig kader:



20109+POL_Beleids
document_BL (1).pdf

Uit het beleidsdocument Online op één lijn:

Social media is voor ons een manier om ons als politie te verbinden met burgers, bedrijven en partners. Via communiceren op social media dragen we bij aan de doelen van de organisatie, het politiewerk en het vertrouwen in de politie.

Pagina 16 beleidsdocument:

4.4 Webcare

Op elk politie account (kwadrant 1 en 2) wordt webcare toegepast. Daarmee moeten alle accounts voldoen aan de afspraken die rondom webcare zijn vastgelegd. Per platform en per kwadrant zijn of worden aparte afspraken gemaakt door het landelijke project webcare in het Webcarekader (onder verantwoordelijkheid van proces Dienstverlening). Voor alle platformen gelden de volgende uitgangspunten:

- Voor elk politie-account op social media is webcare ingeregeld en vastgelegd in afspraken door de beheerder(s) met zijn teamchef en de socialmediaregisseur, gebaseerd op het landelijke Webcarekader.*
- Gefaseerd worden alle accounts aan een webcaretool gekoppeld. Vraag bij je social mediaregisseur na hoe je account gekoppeld moet worden aan de webcaretool en hoe de afspraken over beantwoording in jouw eenheid lopen.*

¹ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

• *Ambitie is om vragen van burgers binnen een uur te beantwoorden, het streven is binnen 24 uur. Op die manier verbinden we ons conform de dienstverleningsovereenkomst daadwerkelijk aan wijk, web, wereld en zijn we bereikbaar en voorspelbaar. Indien webcare op een account niet (meer) haalbaar is, voldoet het account niet aan de gestelde kaders in paragraaf 4.1; en mag je het account (nog) niet opstarten. De webcaretool is niet geschikt voor alle socialmedia-kanalen. Voor Twitter, Facebook en Instagram werkt deze het beste, maar met beperkingen.*

10. Verwerkingstermijnen

Bepaal de verwerkingstermijnen van de politiegegevens aan de hand van de gegevensverwerking en de verwerkingsdoeleinden. Let hierbij op de verschillende verwerkingstermijnen van artikel 8, 9 en 10 Wpg. Beschrijf wie toeziet op de termijnen van verwijderen en de mogelijke vernietiging of archivering aan het einde van de termijnen. Voeg aanvullende informatie toe in het tekstveld.

Gegevensverwerking	Verwerkingsdoeleinden	Soort en Type Politiegegevens	Verwerkings-termijnen en de naleving daarvan	Wie ziet toe op de naleving?
Meldingen, klachten, tips met de daarin gegevens informatie en persoonsgegevens.	Zie onder hoofdstuk 4.	Alle informatie en persoonsgegevens van individuele meldingen van personen worden per melding verwijderd	Gegevens / berichten van burgers worden na 30 maanden automatisch verwijderd.	Automatisch ingesteld in de webcaretool OBI4wan.

Aanvullende informatie over de verwerkingstermijnen:

De termijn van 30 maanden voor het bewaren van berichten is gebaseerd op ervaring uit de praktijk, waarbij het:
a. regelmatig gebeurt dat de beantwoording van berichten een langere doorlooptijd kennen als gevolg van wedervragen.
b. in verband van management rapportages over aantallen en typen berichten (vraag, melding, spoedbericht enz.).

B. Beoordeling rechtmatigheid gegevensverwerking

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de (voorgenomen) gegevensverwerking rechtmatig is. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerking. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen.

11. Doeleinden / wettelijke grondslag.

Bepaal op welke doeleinden de gegevensverwerking wordt gebaseerd. Alle doeleinden moeten aan bepaalde voorwaarden voldoen, voeg in de toelichting op de doeleinden toe hoe aan deze voorwaarden wordt voldaan. Voeg aanvullende informatie toe in het tekstveld.

De doeleinden zijn:

- Artikel 8 Wpg (uitvoering van de dagelijkse politietaken)
- Artikel 9 Wpg (onderzoek i.v.m. de handhaving van de rechtsorde in een bepaald geval)
- Artikel 10 Wpg (inzicht betrokkenheid van personen bij:
 - a) het beramen of plegen van misdrijven²;
 - b) bepaalde ernstige bedreigingen van de rechtsorde³;
 - c) ernstige schending van de openbare orde⁴.)

² Artikel 10 lid 1 onder a jo. Lid 2 Wpg.

³ Artikel 10 lid 1 onder b jo. Lid 3 Wpg.

⁴ Artikel 10 lid 1 onder c jo. Lid 4 Wpg.

- Artikel 12 Wpg (informanten)
- Artikel 13 Wpg (ondersteunende taken)

Let hier ook extra op de verdere verwerkingen o.g.v. artikel 8, 9 en 10 Wpg.

Gegevensverwerking	Doeleinden/wettelijke grondslag	Toelichting op de doeleinden
Informatie van burgers die de Politie ontvangt via de privé Social Media kanalen van de burgers met meldingen, tips, klachten of andere informatie	Artikel 8 Wpg, uitvoering van de dagelijkse politietaken, communicatie met de burgers in het kader van de Politietaken handhaving Openbare Orde en Veiligheid.	

Aanvullende informatie over de doeleinden:

12. Bijzondere politiegegevens

Het verwerken van bijzondere politiegegevens vindt slechts plaats wanneer dit onvermijdelijk is voor het doel van de verwerking, een aanvulling is op de verwerking van andere politiegegevens betreffende de persoon en de gegevens afdoende zijn beveiligd⁵.

Gegevensverwerking	Categorie bijzondere politiegegevens	Toetsing vereisten artikel 5 Wpg
Informatie van burgers die de Politie ontvangt via de privé Social Media kanalen van de burgers met meldingen, tips, klachten of andere informatie. Het kan voorkomen dat betrokkenen gevoelige informatie of bijzondere persoonsgegevens delen vanuit het Social Media kanalen met de Politie via OBI4wan in de vorm van bijvoorbeeld een kopie paspoort, foto's, informatie over derden of bijzondere persoonsgegevens zoals bijvoorbeeld medische kenmerken.	De informatie van burgers kan betreffen: gegevens waaruit ras, etnische afkomst, politie opvattingen, religieuze of levensbeschouwelijke overtuiging, waaruit lidmaatschap van een vakbond blijkt, gegevens over gezondheid, seksuele leven en seksuele gerichtheid (artikel 5 Wpg).	Burgers doen via de genoemde Social Media kanalen zelf een melding en geven daarbij informatie. Deze informatie kunnen bijzondere persoonsgegevens bevatten. Het is niet mogelijk om deze bijzondere persoonsgegevens uit de berichten te filteren. Daarbij is het mogelijk dat de bijzondere persoonsgegevens juist de ken

Aanvullende informatie over de bijzondere politiegegevens:

⁵ Artikel 5 Wpg.

13. artikel 13 ondersteunende taken

Als de politiegegevens voor ondersteunende taken op grond van artikel 13 worden verwerkt, beoordeel of deze verdere verwerking in lijn is met de Wpg en of er is voldaan aan het noodzakelijkheids criterium van artikel 3 Wpg.

Gegevensverwerking	Politiegegevens	Juridische grondslag	Onderbouwing verdere verwerking
Meldingen, klachten, tips, verzoeken van burgers ingediend via hun eigen Social Media kanalen Facebook, Twitter of Instagram.	Naam, accountnaam, inhoudelijke gegevens m.b.t. de melding, verzoek enz.	Artikel 8 Wpg	Op basis van de inhoud van de melding/informatie worden de persoonsgegevens verder verwerkt voor een spoedactie via de meldkamer of doorgezet naar de betreffende eenheid, afdeling voor verdere actie die gebaseerd is op de inhoud van de melding van de burger.

Aanvullende informatie over de ondersteunende taken:

--

14. Noodzaak en evenredigheid

Beoordeel of de voorgenomen verwerking, verstrekking en ter beschikking stelling noodzakelijk en evenredig zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op:

- a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de politiegegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?

Antwoord:

Er worden alleen gegevens verwerkt die verstrekt worden door de burgers zelf via hun eigen Social Media kanalen en accounts. Deze vorm van communicatie met de Politie is een laagdrempelige, efficiënte en effectieve manier voor burgers om meldingen, klachten e.d. aan de Politie door te geven.

In deze GEB is al eerder beschreven en geciteerd uit het beleidsdocument Online op een lijn wat de voordelen zijn voor burgers en de Politie van het gebruik van deze laagdrempelige communicatiemiddelen.

Gezien de procedures van afhandeling en de vertrouwelijke omgang met de gegevens en beveiliging van de betreffende applicatie OBI4wan is er geen sprake van een inbreuk op de persoonlijke levenssfeer en de bescherming van de informatie en politiegegevens van betrokkenen. Het maakt een efficiënte en effectieve vorm van communicatie voor de Politie mogelijk en een snelle beantwoording van vragen voor de burger.

Door het communiceren via de eigen Social Media accounts van de burgers, ligt de verantwoordelijkheid voor het delen van de informatie bij de burger.

- b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt?

Antwoord:

De burger neemt het initiatief welke informatie zij willen delen met de politie. Het is een voor de burger laagdrempelige en makkelijke manier, naast die van telefoon of mail, om te communiceren met de Politie. OBI4wan speelt in op de behoefte van burgers om te werken met de mogelijkheden die Social Media biedt en daarbij gebruik maakt van de eigen Social Media kanalen, die de burgers gebruiken, vergelijkbaar met eigen mailadressen.

Door de grote omvang van het aantal Social Media accounts van de Politie, ruim 2000, biedt de applicatie OBI Engage de Politie een digitale tool voor een snelle, efficiënte en effectieve manier van beantwoording van vragen van burgers of het verder handelen op berichten van burgers.

Indien er niet met OBI Engage gewerkt wordt, wordt een belangrijk 'hedendaags' communicatiekanaal (Social Media) van burgers onbenut gelaten en kan dit voor burgers een belemmering vormen in de communicatie met de Politie. Gelet op de ontwikkelingen in de maatschappij (steeds meer gebruik van Social Media) en de grote schaal van berichten van burgers, leidt het uitschakelen van deze applicatie direct tot vertraging en kwaliteits-terugval in de communicatie met de burger.

15. Rechten van betrokkenen

Binnen de politie is een vaste procedure voor de uitvoering van rechten van betrokkenen. Beschrijf hoe uw organisatie onderdeel uitvoering geeft aan de rechten van de betrokkenen als een verzoek wordt gedaan. Beschrijf op welke wijze organisatorisch is ingericht om te voldoen aan een verzoek van een betrokkene. Beschrijf ook op welke wijze het systeem is ingericht om aan een dergelijk verzoek te voldoen.

Rechten vanbetrokkene	Procedure ter uitvoering	Beperking op grondvan wettelijke uitzondering (artikel 27 Wpg)
Recht op informatie (artikel 24a en 24b Wpg)	Verzoek indienen via de voorziening op de website.	De Politie werkt met een algemene privacyverklaring waarin informatie wordt gegevens over het verwerken van persoonsgegevens. Van burgers.
Recht op inzage (artikel 25 lid 1 Wpg)	Idem	Beperking kan mogelijk zijn, afhankelijk van de inhoud van een bericht, op grond van artikel 27 Wpg.
Recht op rectificatie (artikel 28 lid 1 Wpg)	Idem	
Recht op vernietiging (artikel 28 lid 2 Wpg)	Idem	
Recht om een klacht in te dienen bij de AP (artikel 31a Wpg)	Idem	Niet mogelijk om in te perken.

Beschrijving:

De betrokkenen in de zin van artikel 4, lid 1 van de AVG en artikel 1, onder g van de Wpg hebben de navolgende rechten ten aanzien van de verwerking van hun gegevens.

Op basis van de Wpg hebben zij het recht:

- van inzage;
- van rectificatie, vernietiging of afscherming;
- een klacht indienen zowel bij de organisatie maar ook bij de Autoriteit Persoonsgegevens (AP);

De beslissingen op verzoeken van betrokkenen zijn besluiten in de zin van de Algemene wet bestuursrecht (Awb). Die wet geeft het recht om in beroep tegen een genomen besluit te gaan.

Opvolging geven aan verzoeken van betrokkenen die hun rechten uitoefenen, worden met behulp van bestaande afhandelingsprocessen uitgevoerd via de voorziening (loket) die de Politie daartoe heeft en toegankelijk is via de website en voor medewerkers via intranet. Deze portal en procedure vallen buiten de scope van deze GEB OBI4wan.

Wel binnen de scope valt de bijdrage van OBI4wan/OBI Engage aan het uiteindelijk kunnen afhandelen van verzoeken waar met succes een beroep op is gedaan en gevolgen hebben voor de gegevens zoals zij in OBI4wan zijn opgenomen.

Daarbij gaat het in het bijzonder om de beperking van verwerkingen en vernietiging op basis van de Wpg, welke na onderzoek en op aangeven van de hiervoor genoemde voorziening of de privacyfunctionaris, via de (functioneel) beheerfunctie die de organisatie op dit punt heeft, uitgevoerd moet worden.

Voor wat betreft transparantie wordt naar aanleiding van de beoordeling gesteld dat in de huidige privacy uitingen (in het bijzonder de privacyverklaring die de politie hanteert geen aanvullingen of wijzingen doorgevoerd hoeven worden.

Indien voor OBI Engage geautoriseerde medewerkers een verzoek op grond van de Avg hebben waaronder, recht op inzage, verwijdering, correctie kunnen zij hiervoor een verzoek indienen aan de Korpsleiding. Dit verzoek zal worden behandeld volgens de daarvoor ingerichte procedures binnen de politieorganisatie.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de (voorgenomen) gegevensverwerking voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de voorgenomen gegevensverwerking.

16. Risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

- Welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, zoals het verbod op discriminatie;
- De oorsprong van deze gevolgen;
- De waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
- De ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Gebruik voor de inschatting van de kans, impact en het risico de niveaus 'laag', 'gemiddeld', 'hoog' en 'kritisch'. De kans wordt bepaald aan de hand van de formule kans x impact. Gebruikmaken van de bijbehorende kleuren is aan te raden.

Beschrijving van de risico's:

--

De privacy risico analyse Wpg

De privacy risicoanalyse is gebaseerd op het model DPIA rijksdienstmodel 2021. Het maakt onderdeel uit van het format GEB-formulier Wpg. Het gaat bij privacy risico's primair om de gevolgen voor de betrokkene. Naast de risico's voor de betrokkene bestaan er ook risico's voor de organisatie.

Voor de inschatting van de risico's wordt onderstaande risicomatrix toegepast. Het tweede deel bestaat uit de geadviseerde maatregelen en een inschatting van het restrisico voor en na het nemen van mitigerende maatregelen. De risico's en maatregelen zijn in overeenstemming met de Wpg bijv. met betrekking tot de doelen van de verwerking en de verwerking van bijzondere gegevens. Onder gegevens wordt verstaan politiegegevens in de zin van artikel 1 Wpg.

Risicomatrix verwerkingen Wpg

Impact					
	1. Verwaarloosbaar	2. Minimaal	3. Gemiddeld	4. Maximaal	5. Kritisch
Kans	5. Zeer groot (wekelijks, het treedt al op)	5 MEDIUM	10 MEDIUM	15 HOOG	20 KRITISCH
	4. Groot (maandelijks)	4 MEDIUM	8 MEDIUM	12 HOOG	16 HOOG
	3. Gemiddeld (jaarlijks)	3 LAAG	6 MEDIUM	9 MEDIUM	12 HOOG
	2. Klein (eens in de 5 jaar)	2 LAAG	4 LAAG	6 MEDIUM	8 MEDIUM
	1. Zeer klein (5 jaar+)	1 LAAG	2 LAAG	3 LAAG	4 MEDIUM
Impact					
	1. Verwaarloosbaar	2. Minimaal	3. Gemiddeld	4. Maximaal	5. Kritisch
Privacy	Zeere kleine kans op schending beschikbaarheid, integriteit of vertrouwelijkheid van persoonsgegevens .	Minimale schending beschikbaarheid, integriteit of vertrouwelijkheid algemene persoonsgegevens (NAW, email, telnr.)	Schending beschikbaarheid, integriteit of vertrouwelijkheid algemene en/of te relateren aan een overtreding, persoonsgegevens.	Grootschalige schending beschikbaarheid, integriteit of vertrouwelijkheid algemene persoonsgegevens en bijzondere persoonsgegevens of persoonsgegevens te relateren aan een misdrijf.	Grootschalige schending beschikbaarheid, integriteit of vertrouwelijkheid algemene persoonsgegevens en bijzondere persoonsgegevens of persoonsgegevens te relateren aan een ernstig misdrijf.

Risico analyse privacy issues Wpg verwerkingen

Categorieën	Geconstateerde privacy issues/risico's	Kans	Impact	In-schatting
1. Organisatie				
Verwerkings-verantwoordelijke	Er is geen duidelijke verwerkingsverantwoordelijke	1	1	Verwaarloosbaar
Rechtmatigheid	De verwerking valt niet onder een van de doelen van de Wpg of voldoet niet aan een van de eisen van de Wpg.			Idem
Werkproces	De verwerking heeft geen beschreven of een verouderd werkproces in de bedrijfsarchitectuur.			Idem
Transparantie	De verwerking is niet inzichtelijk geworden waardoor oa. de rechten betrokkenen niet of gedeeltelijk uitgevoerd kunnen worden.			Idem
Uitvoering	De verwerking wordt in de eenheden niet uniform uitgevoerd.			Idem
Autorisatie	Er is geen autorisatiebeleid of autorisatiematrix voor deze verwerking.			Idem
verwerkingstermijnen	De verwerkingstermijnen worden niet nageleefd.			idem
Overig:				
2. Mens				
Kennis	De functionarissen blijken niet of onvoldoende op de hoogte van de privacyregels.	1	1	Verwaarloosbaar
Screening	De functionarissen beschikken niet over het juiste screeningsniveau.			Idem
Overig:				
3. Gegevens				
Noodzakelijk	Er worden politiegegevens verwerkt die niet noodzakelijk zijn voor de wettelijke doeleinden.	3	1	laag
Big data	De regels voor big data verwerking worden niet nageleefd			Niet aan de orde
Proportionaliteit	Er worden teveel gegevens verwerkt	3	1	Laag
Proportionaliteit	Er zijn geen condities gesteld aan de vrije tekstvelden.	1	1	Verwaarloosbaar. Is de kern van de applicatie voor berichten van burgers.
Subsidiariteit	Er zijn andere voor de betrokkene minder ingrijpende maatregelen mogelijk.	1	1	Verwaarloosbaar
Betrokkenen	Er wordt geen duidelijk onderscheid gemaakt in de verwerking tussen verschillende categorieën van betrokkenen: verdachten, slachtoffers, derden.	1	1	Verwaarloosbaar
Bijzondere politiegegevens	Er wordt niet voldaan aan de drie wettelijke eisen van de Wpg voor de bijzondere politiegegevens: onvermijdelijk voor het doel, in aanvulling op andere politiegegevens, zijn afdoende beveiligd.	1	1	Verwaarloosbaar
ID nummers	Er is geen grondslag om een wettelijk ID nummer te verwerken.	1	1	Verwaarloosbaar
Verdere verwerking	De politiegegevens worden voor andere doelen verder verwerkt zonder toetsing vooraf volgens de Wpg.	1	1	Verwaarloosbaar
Ter beschikkingstelling	De applicatie A, B, of C zijn gekoppeld met andere applicaties zonder dat hiervoor toestemming is of de data getoetst zijn op proportionaliteit en noodzaak voor interne verstrekkingen.	1	1	Verwaarloosbaar
Datakwaliteit	De kwaliteit van de gegevens wordt niet gecontroleerd of is niet voldoende.	1	1	Verwaarloosbaar

Categorieën	Geconstateerde privacy issues/risico's	Kans	Impact	In-schatting
Output	Het is niet overzichtelijk welke output wordt gegenereerd uit de verwerking en wie daar toegang toe heeft.	1	1	Verwaarloosbaar
Minderjarig	Het is mogelijk dat minderjarigen via hun Social Media accounts informatie delen met de Politie via OBI4wan.	3	1	laag
Overig:				
4. Technische aspecten				
Doel applicatie	De applicatie A, B, wordt voor meerdere doelen gebruikt.	1	1	Verwaarloosbaar
	De koppelingen met andere systemen zijn niet duidelijk.	1	1	Verwaarloosbaar
IB analyse				Uitgevoerd zie onder hoofdstuk 17 OBI4wan voldoet aan ISO27001
Logging				Er vindt logging plaats op de activiteiten in OBI4wan.
e-mail	Er worden politiegegevens zonder afdoende beveiligde e-mail naar externe partners verzonden.			Er wordt gebruik gemaakt van Politie-mail.
Overig:				
5. Externe partijen				
Grondslag	De verstrekking aan derden wordt niet gelegitimeerd door een van de wettelijke mogelijkheden.	1	1	verwaarloosbaar
Convenant	Voor een gezamenlijke gegevensverwerking ontbreekt een convenant of er is een onvolledig convenant.	1	1	verwaarloosbaar
Contractuele afspraken	Er ontbreken afspraken met de leverancier of een andere externe partij over de verwerking van politiegegevens en de informatiebeveiliging.	1	1	Verwaarloosbaar (er is een leveranciersovk, deze wordt met een productgericht uitvraag verlengd)
Verwerker	Het is niet duidelijk of de betrokken externe partij verwerker is.	1	1	Verwaarloosbaar
Verwerkers-overeenkomst	Er ontbreekt een verwerkersovereenkomst of deze volgt niet het model van de politie.	1	1	Verwerkersovereenkomst wordt afgesloten na gunning.
Geheimhoudingsplicht	De externe partij is niet op de hoogte van de geheimhoudingsplicht ogv de Wpg.	1	1	Verwaarloosbaar
Cloudopslag	De verwerking in de cloud voldoet niet aan de informatiebeveiligingseisen.			CIO oordeel wordt aangevraagd voorafgaand aan de productgericht uitvraag.
Verwerking buiten EER		1	1	Verwaarloosbaar (zie verwerkersovk.)
Wetenschap	De verstrekking voor beleidsinformatie, wetenschappelijk onderzoek of statistiek heeft ten onrechte geleid tot resultaten met persoonsgegevens.			Niet aan de orde
Overig:				

D. Maatregelen en restrisico's

In onderdeel D wordt geadviseerd welke maatregelen getroffen kunnen worden om de geconstateerde risico's uit onderdeel C naar een aanvaardbaar niveau te brengen. Risico's volledig reduceren is (vaak) niet mogelijk. Dit betekent dat er altijd een resterend risico zal overblijven. De verwerkingsverantwoordelijke dient te beschrijven hoe het tot dit restrisico is gekomen en waarom deze aanvaardbaar wordt geacht.

17. Maatregelen

Een passend beveiligingsniveau veronderstelt dat gewerkt wordt met een planning- en controlcyclus (plan-do-check-act) aan de hand waarvan kan worden beoordeeld of de beveiliging steeds adequaat is voor de huidige stand van de techniek en de organisatie.

Voor te treffen maatregelen kan worden aangehaakt bij beveiligingskaders en -standaarden, beste praktijken en goedgekeurde gedragscodes en certificeringsmechanismes. Wanneer een of meerdere van toepassing zijn op de gegevensverwerkingen, beschrijf dan specifiek welke beveiligingsstandaarden, praktijken, gedragscodes en/of certificeringsmechanismes van toepassing zijn en op welke manier deze in de praktijk van toepassing zijn op de gegevensverwerkingen. Bij het bepalen van de gepaste maatregelen moet ook rekening gehouden worden met maatregelen die voortvloeien uit de Baseline Informatiebeveiliging Overheid (BIO).

IB-analyse

In 2019 is een IB-analyse uitgevoerd voor OBI Engage. Van de aanbevelingen om risico's te mitigeren zijn er inmiddels een aantal uitgevoerd en enkele zijn in uitvoering.

Uitgevoerd zijn:

- weghalen van de autorisatie bij de superuser om een nieuwe gebruiker aan te maken voor OBI. Deze zit alleen nog op het niveau van een Eenheidsbeheerder en Toplevelbeheerder.
- De aanbeveling om alle nieuwe aanvragen voor een OBI inlog te laten registreren via de ATL is in gang gezet. Zal in Nov 2022 gerealiseerd zijn.
- 2FA is beschikbaar in 2023. Opgenomen in Roadmap van 2023 OBI. Benodigde budget binnen de politie aangevraagd. Met leverancier OBI4wan is er overleg om dit onderdeel in Q1 van 2023 uit te voeren.
- Aanbeveling voor de trainingen: trainingsomgeving voor OBI Engage is aangekocht en is 1-1-2023 operationeel om politiemedewerkers te trainen in het werken met OBI Engage.

Het contract voor de applicatie OBI Engage wordt verlengd met een periode van 5 jaar.

De komende jaren zal verder gewerkt worden aan het realiseren van de mitigerende maatregelen.

De mitigerende maatregelen voor een, conform de IB-analyse en -aanbevelingen verwerking, dienen te worden opgepakt door de verwerkingsverantwoordelijke zelf.

De maatregelen voor de ondersteunende systemen worden reeds opgepakt. Meer gedetailleerde informatie hierover in de hieronder toegevoegde beveiligingsanalyse en technische uitgangspunten OBI Engage.



Beveiligingsanalyse
OBIengage 1_0.doc



PHDPCSUP-OBIEng
age-290922-1240-10



GEB registreren in
JIRA.docx

Maatregelen getroffen door leverancier OBI4wan m.b.t. de applicatie OBI Engage

OBI4wan is een SaaS-oplossing en dat betekent dat alle gegevens via een internetverbinding worden verwerkt en opgeslagen via een beveiligde verbinding op de servers in de datacentra van OBI4wan in Nederland.

Alle data wordt binnen de EU/EER opgeslagen.

Opdrachtnemer OBI4wan en diens sub-verwerker zijn in het bezit van een geschreven beveiligingsbeleid conform ISO 27001 inzake Information Security Management.

De organisatorisch en technische beveiligingsmaatregelen die de leverancier treft omvatten in ieder geval:

- a. Maatregelen om te waarborgen dat enkel bevoegd Personeel van Opdrachtnemer toegang heeft tot de Persoonsgegevens en/of Politiegegevens voor het doel dat is uiteengezet in Bijlage 1 van de Verwerkersovereenkomst;
- b. Maatregelen waarbij Opdrachtnemer zijn Personeel en Hulpverleners uitsluitend toegang geeft tot Persoonsgegevens en/of Politiegegevens via op naam gestelde accounts, waarbij het gebruik van die account adequaat gelogd wordt en waarbij de betreffende account alleen toegang geven tot die Persoonsgegevens en/of Politiegegevens waartoe de toegang noodzakelijk is;
- c. Maatregelen om de Persoonsgegevens en/of Politiegegevens te beschermen tegen onopzettelijk of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, verwerking, toegang of openbaarmaking;
- d. Maatregelen om zwakke plekken te identificeren ten aanzien van de verwerking van Persoonsgegevens en/of Politiegegevens in de systemen die worden ingezet voor het verlenen van de diensten aan de Politie;
- e. Maatregelen om de tijdige beschikbaarheid van de gegevens te garanderen die benodigd zijn voor het uitvoeren van de Overeenkomst.

Risico	Maatregelen	Restrisico na maatregel	Beheerder van de maatregelen
2F-Authenticatie is nog niet gerealiseerd.	2FA is beschikbaar in 2023. Opgenomen in Roadmap van 2023 OBI. Benodigde budget binnen de politie aangevraagd. Met leverancier OBI4wan is er overleg om dit onderdeel in Q1 van 2023 uit te voeren.	Er wordt in de operatie gewerkt met OBI Engage, zonder een 2FA. Ook bij een verlenging van het contract per 1 januari 2023 zal dit nog niet zijn gerealiseerd.	Verwerkingsverantwoordelijk portefeuillehouder,

Onderbouwing acceptatie restrisico's:

2FA is beschikbaar in 2023. Opgenomen in Roadmap van 2023 OBI. Benodigde budget binnen de politie aangevraagd. Met leverancier OBI4wan is er overleg om dit onderdeel in Q1 van 2023 uit te voeren.