Versiebeheer en ondertekening

Datum: 25-1-2021

Opdrachtgever BSN.FIJ

Versies

Versie	Datum	Auteur	Samenvatting van de wijzigingen
0.1	2-4-2019	5.1,2E	Eerste conceptversie
1.0	18-7-2019	5.1,2E 2e	Gehele DPIA doorgenomen en aanscherpingen aangebracht

Adviezen belangrijkste stakeholders

Versie	Datum	Stakeholder	Advies
1.0	23-7-2019	5.1,2E)	De DPIA bevat veel juridisch jargon en juridische beschrijvingen. Inwoners zijn een belangrijke doelgroep en het document moet voor hen goed leesbaar zijn.

Reactie proceseigenaar op advies

Versie	Proceseigenaar	Reactie / wijze van opvolging
1.0	5.1,2E	Separate samenvatting gemaakt op B1 niveau

Goedkeuring / vaststelling

Versie	Datum	Naam	Ondertekening
1.0		Patrick van Doorn, Hoofd Juridische Zaken en Aanbesteding	Patrick van Doorn on 25-01-2021

Gemeente Utrecht

Data protection impact assessment (DPIA)

Uitwerking artikel 35 van de Algemene verordening gegevensbescherming EU 679/2016

Gemeente Utrecht / [BSN] / [JZI]

[project geautomatiseerd anonimiseren en ontdubbelen]

Versie: 1.0

Bron: DPIA model van Verdonck, Klooster & Associates en het DPIA model van de Rijksoverheid

Voorbereiding: Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

1. Voorstel
Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en de context waarbinnen deze plaatsvindt op hoofdlijnen.
De overheid moet in het kader van haar wettelijke taken regelmatig informatie anonimiseren voordat documenten kunnen worden verstrekt of ter inzage kunnen worden gelegd. Het gaat daarbij om werkprocessen zoals de bestuurlijke besluitvorming (agendapunten raadsvergadering), de AVG, inzage verzoeken in het kader van handhaving of bijstand, inzage in bezwaardossiers Awb (Algemene wet bestuursrecht), inzage verkeersboetedossier Wahv (Wet administratiefrechtelijke handhaving verkeersvoorschriften) en natuurlijk de Wob (Wet openbaarheid van bestuur). Daarnaast houdt de gemeente een aantal balies bij waar om openbare informatie wordt verstrekt aan een ieder, zoals de balie Bouwen en Woning (vergunningen) en het Horecaloket (Drank- en Horeca ontheffingen). Elk werkproces kent zijn eigen regels van welke persoonsgegevens wel en welke persoonsgegevens niet zichtbaar mogen zijn. Ter illustratie is hoe de Wob en Wob jurisprudentie aangeeft hoe moet worden omgegaan met persoonsgegevens. Wob kent een bijzondere regeling op het vlak van het openbaarmaking van persoonsgegevens. Bijzondere persoonsgegevens mogen niet openbaar worden gemaakt. Algemene persoonsgegevens mogen worden afgewogen tegen het belang van openbaarmaking. Bij de Wob is door de rechter bepaalt dat - bij belangenafweging - derden recht hebben op volledige privacy, met uitzondering van verplichte registraties in openbare bronadministraties of uit eigen beweging openbaar gemaakte persoonsgegevens, zoals een contactpersoon voor werkzaamheden van Eneco in Ondiep op de website van Eneco. Voor ambtenaren geldt dat die maar beperkt recht hebben op privacy (een ambtenaar is een verlengde van het “openbaar” bestuur. Het openbaar bestuur is aanspreekbaar en verantwoordelijk voor zijn handelen, een anonieme overheid bestaat niet) . Een ambtenaar die een functie naar buiten toe vervult, zoals een directeur met mandaat en de verplichting om zijn naam en handtekening onder een besluit te zetten of communicatieadviseur (namen zijn al openbaar gemaakt via website), blijft staan in de tekst conform de jurisprudentie op dit vlak. De persoonsgegevens van ambtenaren die geen functie naar buiten toe vervullen (beleidsmedewerker, administratief medewerker) worden onleesbaar gemaakt. Dit betekent dat per Wob-dossier een gedetailleerde screening van persoonsgegevens moet plaatsvinden. In het wetsvoorstel Wet open overheid wordt het categorisch openbaar maken van diverse categorieën van documenten, zoals vergunningen, convenanten en klachten een wettelijke taak. Het anonimiseren van persoonsgegevens gebeurt nu handmatig met een applicatie. Deze werkwijze is potentieel foutgevoelig. Je moet tijdens de verwerking lijsten bijhouden van namen die wel en namen die niet openbaar mogen zijn (naar mate de lijst langer wordt, wordt het steeds ingewikkelder en de kans op fouten groter). Daarnaast komt het regelmatig voor dat soms een naam weer leesbaar moeten worden gemaakt. Dan moet je bladzijde voor bladzijde alle rode kaders verwijderen. We zijn daarom op zoek gegaan naar een tool die het mogelijk maakt om eenvoudig namen in het gehele dossier in één keer te markeren met menselijke eindcontrole. Het is nooit 100%, dus de behandelend ambtenaar moet de volledige tekst, net als nu, checken om te kijken wat de software heeft gemist. Doordat de software al een groot deel van de persoonsgegevens heeft voorzien van een kleur gaat het controleren eenvoudiger en is het toevoegen of verwijderen van een naam in het hele dossier maar één handeling in plaats van tientallen rode kaders toevoegen of verwijderen. Sinds oktober vorig jaar hebben we een applicatie met de mogelijkheid om geautomatiseerd bestanden chronologisch te ordenen, te ontdubbelen en ook te anonimiseren. De software herkent technisch aan de hand van markers (een aangewezen plek op een document (zoals een regel in een e-

formulier waar iemand de persoonsgegevens invult, onder Hoogachtend staat meestal een handtekening of alle teksten voor @utrecht.nl)) waar mogelijke persoonsgegevens zitten. De behandelaar moet die vervolgens stuk voor stuk checken, accepteren en de persoonsgegevens die gemist zijn handmatig toevoegen.

2. Persoonsgegevens

Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van betrokkene aan welke persoonsgegevens van hen verwerkt worden. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificatienummer. Maak gebruik van het bijgevoegde overzicht van soorten persoonsgegevens.

Het gaat alle vormen van persoonsgegevens die de overheid gevraagd of ongevraagd ontvangt:

- NAW-gegevens;
- Contactgegevens (e-mail berichten, telefoonnummers);
- Herleidbare gegevens zoals “ik woon in het hoekhuis met de rode garagedeur”
- Kenttekens
- BSN-nummers
- Bijzondere persoonsgegevens over lidmaatschap vakbond, seksuele leven, strafrechtelijk verleden
- foto’s;
- scans van identiteitsbewijzen

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

Het anonimiseren van (een deel van de) persoonsgegevens conform daarvoor geldende wettelijke grondslag in brongegevens die door organisatieonderdelen worden aangeleverd of klaar gemaakt voor inzage, openbaarmaking of verstrekking, inclusief ontdubbelen en chronologisch ordenen.

4. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Het creëren van een geanonimiseerd dossier/stukken wat conform de daarvoor geldende wettelijke grondslaggeschikt is voor inzage, openbaarmaking of verstrekking aan een verzoeker.

5. Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

Gemeente Utrecht is in dit geval verwerkingsverantwoordelijke. De daadwerkelijk verwerking vindt plaats door de behandelend ambtenaar . Die beoordeelt welke gegevens onleesbaar moeten worden gemaakt. Die sleept de bronbestanden naar de map, haalt ze door de software heen en controleert het voorwerk.

Er is één functioneel beheerder die technische vragen beantwoord en eventuele technische problemen kan oplossen. Deze beheerder heeft geen inzagerechten noch kan bewerkingen uitvoeren of controleren, die een behandelend ambtenaar uitvoert tenzij de behandelend ambtenaar iemand van PLC erbij haalt en laat meekijken achter het scherm.

Deze software draait volledig intern op gemeentelijke servers en heeft geen externe toegangen waarmee leveranciers data uitwisselt of toegang heeft tot data.

6. Belangen bij de gegevensverwerkingen

Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

De gemeente kan mogelijk hiermee efficiënter documenten anonimiseren, de factor menselijk fout te verkleinen en eerder de wettelijke beslistermijn halen omdat er minder handwerk hoeft te worden gedaan. Zeker bij de grote Wob-dossiers (veel documenten) lukt het nu niet of moeilijk om binnen de wettelijke termijn te beslissen, omdat het handmatig controleren van teksten, ordenen en ontdubbelen veel tijd kost. Met het wetsvoorstel Wet open overheid, thans is het wijzigingswets-voorstel in behandeling bij de 2e Kamer, gaat de beslistermijn terug naar acht weken naar vier weken.

De verwerker heeft een commercieel belang bij de verwerking.

7. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

In de overeenkomst met de leverancier zal worden opgenomen dat er geen gegevens worden verwerkt buiten de Europese Economische Ruimte.

8. Technieken en methoden van de gegevensverwerkingen

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-) geautomatiseerde besluit-vorming, profilering of big data-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

De tekst in de te anonimiseren documenten zal machine-leesbaar (OCR) worden gemaakt. Vervolgens worden hierin op basis van een algoritme met taaltechnologie de persoonsgegevens herkent en deze worden gemarkeerd met een kleur. Vervolgens moet de behandelend ambtenaar de teksten, inclusief kleren checken en maakt de eindversie op. In de eindversie worden de persoonsgegevens onomkeerbaar geanonimiseerd (de zwarte balken kunnen niet ongedaan worden gemaakt).

9. Juridisch en beleidsmatig kader

Benoem de wet-en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de voorgenomen gegevensverwerkingen.

De Wob verplicht de overheid om bijzondere persoonsgegevens onleesbaar te maken en algemene persoonsgegevens af te wegen tegen het belang van openbaarmaking daarvan. Deze belangenafweging vergt dat gedetailleerd wordt gescreend welke persoonsgegevens onleesbaar moeten worden gemaakt en welke moeten blijven staan.
De Awb verplicht de overheid om ingeval van bezwaar een bezwaardossier ter inzage te leggen of op verzoek een kopie daarvan te verstrekken. Als er meer bezwaarden zijn moeten de persoonsgegevens van de andere bezwaarden onleesbaar worden gemaakt. Ook eventuele zienswijzen die in het vergunningendossier zitten mogen leesbaar zijn als het gaat om dezelfde persoon, maar van andere personen mogen die gegeven niet verstrekt worden.
Ook bij verkeersboetedossiers op grond van de Wahv kan iemand die een boete heeft ontvangen zijn eigen dossier opvragen, maar worden persoonsgegevens van de behandelend ambtenaar onleesbaar gemaakt.
Bij AVG verzoeken moeten persoonsgegevens van andere burgers onleesbaar worden gemaakt. De persoonsgegevens van de verzoeker blijven wel staan.
Ook bij inzageprocedures in het kader van de bijstand of handhavingstrajecten worden eigen gegevens leesbaar gelaten en persoonsgegevens van anderen onleesbaar gemaakt.

10. Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

De verstrekte documenten worden opgeslagen in het daarvoor geldende zaaktype (Wob) of geautomatiseerde systeem waar de primaire taak mee wordt uitgevoerd. Daarvoor geldt volgens de VNG richtlijnen een bewaartermijn (bijvoorbeeld voor de Wob is dat één jaar). Bij inzagetrajecten kan na inzage de set worden verwijderd of ingeval van de Awb bezwaarprocedure kan alleen een bepaalde

periode voor de hoorzitting om inzage of verstrekking worden gevraagd. Voor gepubliceerde Wob-dossiers geldt dat ze na verloop van een jaar verwijderd, omdat de content actueel moet zijn en oude dossiers geen informatiewaarde meer hebben.
De verkenner mappen met originele Wob-brondocumenten worden 3 jaar bewaard in verband met aansprakelijkheidsclaims en ten behoeve van reconstructiedoeleinden.

Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel de rechtsgrond, noodzaak en doelbinding van de voorgenomen gegevensverwerkingen en rechten van de betrokkene.

11. Rechtsgrond
Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd. Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dit is toegestaan.
Het gaat hier om de grondslag wettelijke verplichting op basis van wetten zoals de Wahv, de AVG, de Awb en de Wob. Het inzien, openbaar maken of verstrekken is een secundair proces. Het gaat om persoonsgegevens die op grond van andere primaire processen zijn verzameld.
12. Doelbinding
Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.
Het gaat hier alleen om wettelijke rechten op inzage, verstrekking of openbaarmaking. De persoonsgegevens worden alleen voor dat doel verwerkt. Aanvullend voor de Wob. De Wob is van toepassing op elk document die bij de overheid rust. Daarnaast is het uitgangspunt van de Wob dat alle informatie openbaar is, tenzij één van weigeringsgronden van de Wob zich daar tegen verzet. Als zodanig is het een generieke wettelijk basistaak die van toepassing is op elk document bij de gemeente.
13. Juistheid
Beoordeel de kwaliteit van de te verwerken gegevens.
De behandeld ambtenaar beoordeelt de kwaliteit van de verwerking, kan bepalen of bepaalde gegevens extra moet worden gemarkeerd voor onleesbaar maken of voorgeselecteerde gekleurde teksten de-selecteren zodat ze wel leesbaar zijn. De software doet het voorwerk. De behandelend ambtenaar de eindcontrole zodat de inzage, verstrekking of openbaarmaking voldoet aan de voor die wet geldende regels. Het gaat om een 100% beoordeling (oftewel alleen die persoonsgegevens mogen zichtbaar zijn die ook zichtbaar mogen zijn) . Anders is sprake van een datalek.
14. Noodzaak en evenredigheid
Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit. *a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?* *b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt? Benoem hierbij de overwogen alternatieven.*
Door deze automatisering zullen dezelfde gegevens moeten worden gemarkeerd ten behoeve van anonimisering, als voorheen handmatig wordt gemarkeerd, en verwerkt. Het gaat hier louter om de technische verwerking (markeren en zwart maken zonder ongedaanmakingsmogelijkheid). De inhoudelijke beoordeling en belangenafweging – welke tekstdelen daar wel en niet onder vallen – vindt plaats op grond van de wettelijke grondslag en jurisprudentie.

15. Opslag
Beoordeel of de gegevens van alle verwerkingen niet langer dan noodzakelijk bewaard worden.
De behandelend ambtenaar slaat de met de applicatie verwerkte set op in het daarvoor aangewezen zaaktype of automatiseringssysteem en de daarvoor door de recordmanager bepaalde bewaartermijn. (zie verder onder 10 bewaartermijn).
16. Bescherming
Beoordeel of alleen geautoriseerde medewerkers en externe partners/leveranciers toegang hebben tot de gegevens. Geef op hoofdlijnen en in lekentaal weer hoe de gegevens beschermd zijn tegen ongeautoriseerd gebruik.
De werkmap van de applicatie is alleen toegankelijk voor de geautoriseerde medewerker die een set met documenten daarin sleept. Andere behandelaars of zelfs de technische ondersteuning heeft geen toegang tot de documenten. De coördinator van het Wob-team van IB JZI bepaalt wie autorisatie krijgt om te werken met deze applicatie. Meldt aan en af. Autorisatie worden alleen gegeven aan medewerkers die inzage, verstrekkings- of openbaarmakings-taken uitvoeren. Uitgegeven autorisaties worden periodiek gecontroleerd.
17. Rechten van de betrokkenen
Geef aan hoe invulling wordt gegeven aan de rechten van de betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzondering dat is toegestaan.
Het gaat in bepaalde wetten om het nemen van besluiten (zoals de AVG en de Wob) en in andere wetten om het uitvoeren van feitelijke handelingen, zoals het inzien van een bezwaardossier. Elke wettelijke procedure heeft hiervoor zijn eigen invulling. Inzage van een bijstandsdossier ziet op je eigen gegevens, niet op die van anderen. Bij inzage in vergunningendossiers geldt in veel gevallen dat de aanvrager wel of geen toestemming heeft gegeven om zijn persoonsgegevens te delen. Bij de Wob geldt dat derden onverkort recht hebben op bescherming van hun privacy en voor ambtenaren geldt dat die beperkt recht hebben op bescherming van hun privacy. Per taakveld wordt dit ingevuld.

C. Beschrijving en beoordeling risico's voor de betrokkenen

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

18. Risico's
Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Ga in ieder geval in op: *a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;* *b. de oorsprong van deze gevolgen;* *c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;* *d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.*
Er kan onterecht vertrouwen ontstaan in de mate van anonimisering en ontdubbeling door de software waardoor documenten mogelijk niet integraal worden gecontroleerd. De kans hierop is vrij klein maar de impact aanzienlijk als er sprake is van bijzondere persoonsgegevens. Onbevoegden zouden kennis kunnen nemen van informatie uit documenten als autorisaties niet op orde zijn binnen de interne organisatie. De externe leverancier zou onbedoeld kennis kunnen nemen van vertrouwelijke informatie uit de dossiers, bijvoorbeeld bij functionele of technische gebreken in de software. De kans hierop is klein maar de impact is groot, aangezien de gegevens in een andere context worden verwerkt als waar deze oorspronkelijk vandaan komen en gezien de potentiele gevoeligheid van de betreffende gegevens.

D. Beschrijving voorgenomen maatregelen

Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de voorgenomen gegevens-verwerkingen voor de vrijheden en rechten van de betrokkenen aan te pakken.

19. Maatregelen
Beoordeel of de reeds getroffen maatregelen, beschreven onder '16. Bescherming', afdoende zijn. Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.
Er is altijd een menselijke controle op de aangebrachte markeringen vanwege het gegeven dat geen enkele software foutloos werkt. Persoonsgegevens herkennen en vooral herleidbare gegevens vergt een bepaalde routine en ervaring. Er wordt daarom nadrukkelijk gekeken naar de kwaliteiten van de aanvrager van een account en er worden 'trainingen" verzocht zodat diegenen die ermee gaan werken vaardig zijn om alle handelingen te verrichten. Onbevoegde kennisname of ontvangst van (documenten met) persoonsgegevens blijft een gering restrisico als door een menselijke fout toch bepaalde persoonsgegevens leesbaar zijn die niet leesbaar mogen zijn. Kennisname door onbevoegden binnen onze organisatie wordt uitgesloten door te werken met strikt beheerde autorisaties en de bestaande systemen die aangewezen zijn. Kennisname van onbevoegden in dienst van de leverancier wordt uitgesloten doordat de leverancier geen toegang heeft tot de applicatie zoals deze bij ons draait. De leverancier krijgt ook niet op enige andere manier documenten met persoonsgegevens van ons ter beschikking. Dit wordt bevestigd in een overeenkomst met de leverancier. Onterecht aanwijzen van documenten als dubbelingen door de software wordt in de testfase uitvoerig gecontroleerd.