Privacyhandboek

Gemeente Leiden, Leiderdorp, Oegstgeest, Zoeterwoude & Servicepunt71

Versiedatum	13-11-2018
Versie	Eerste definitieve versie 2.0
Status	Definitief

Inhoudsopgave

Privacyhandboek

De gemeenten Leiden, Leiderdorp, Oegstgeest, Zoeterwoude en hun gezamenlijke bedrijfsvoeringsorganisatie Servicepunt 71 (hierna: de gemeente / Servicepunt 71) hechten grote waarde aan de bescherming van PERSOONSGEGEVENS. Medewerkers van de gemeente / Servicepunt 71 kunnen dit handboek erop naslaan om te lezen wat er van hen verwacht wordt op het gebied van privacy en gegevensbescherming.

Het uitgangspunt van dit privacyhandboek is eenvoudig: *PERSOONSGEGEVENS worden door of namens de gemeente / Servicepunt71 uitsluitend in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG) VERWERKT.*

Bijdragen aan de kwaliteit van het privacyhandboek

Hebben wij je kunnen helpen door het opstellen van dit privacyhandboek? Heb je kunnen vinden wat je zocht of stond de gewenste informatie er niet in? Was het begrijpelijk, of teveel in de taal van de expert? De privacybeheerders zijn constant op zoek naar mogelijkheden om de communicatie omtrent Privacy te optimaliseren. En jij kunt daarbij helpen!

☞ **HEB JE TIPS / AANVULLINGEN / VERBETEREN VOOR DIT PRIVACYHANDBOEK?** GEEF DIT DAN DOOR AAN DE PRIVACYBEHEERDER. EIND 2018 ZAL DIT DOCUMENT VOOR DE EERSTE KEER HERZIEN WORDEN EN DAARIN WORDEN ALLE SUGGESTIES MEEGENOMEN.

Leeswijzer

De onderwerpen die worden behandeld in dit handboek, zijn voorzien van steekwoorden en een kleurcode voor snelle navigatie en herkenbaarheid.

Hoofdstuk	*kleurcode*
1. Algemene omgang met persoonsgegevens Rechtmatigheid, Behoorlijkheid, Transparantie etc.	
2. Nieuwe en gewijzigde verwerkingen Privacy Impact Assessment, Privacy by Design	
3. Doelbinding Testen, verenigbare doelen, hergebruik	
4. Beveiligingsincidenten en datalekken Beveiligingsincident	
5. Beveiliging Passende technische en organisatorische maatregelen	
6. Inschakelen van en doorgifte aan derden Verwerker, ontvanger, gezamenlijke verantwoordelijkheid	
7. Archiveren en vernietigen Vernietiging, bewaartermijn, Archiefwet	
8. Bewustzijn Bewustwording, awareness, training	
9. Rechten van betrokkenen Recht op inzage, recht op vergetelheid	

Dit handboek is hoofdzakelijk bedoeld als een handleiding die medewerkers erop kunnen naslaan om te lezen wat er concreet van hen verwacht wordt in het kader van gegevensbescherming.

De onderwerpen zijn als volgt opgebouwd: voor de AVG-onderwerpen die in dit handboek behandeld worden is een beleidsregel ('uitgangspunt') verwoord. Vervolgens is zo praktisch mogelijk beschreven hoe hier gevolg aan gegeven wordt. Daarna is beknopt opgesomd welke stappen doorlopen dienen te worden. En tot slot is – waar mogelijk – verwezen naar onderwerp-specifieke werkwijzen en procedures. Gepoogd is deze structuur van de hoofdstukken zo visueel en intuïtief mogelijk op te bouwen. Er wordt (waar mogelijk en relevant) steeds gebruikgemaakt van de volgende koppen:

Uitgangspunt
Hier wordt de beleidsregel op hoofdlijnen uiteengezet.

- **Realisatie**
  De wijze waarop de beleidsregel gerealiseerd wordt, wordt hier beschreven. In de meeste gevallen wordt verwezen naar een onderwerp-specifieke werkwijze of procedure. De inhoud daarvan is in sommige gevallen kort samengevat. Nummers tussen haakjes, corresponderen met de bijbehorende instructies (**1**).

✓ (**1**) **Instructies**
Wat er concreet van medewerkers wordt verwacht, is – waar mogelijk – onder dit kopje opgesomd.

☞ **Verwijzingen**
Er wordt veelvuldig verwezen naar onderwerp-specifieke werkwijzen en procedures. Een korte beschrijving en de vindplaats zijn onder dit kopje opgenomen.

Verantwoordelijkheden

[**R**]esponsible [**A**]ccountable [**C**]onsulted [**I**]nformed	
R	Wie is er verantwoordelijk voor het juist uitvoeren van deze beleidsregel?
A	Wie is er eindverantwoordelijk voor het juist uitvoeren van deze beleidsregel?
C	Wie moet geraadpleegd worden voor het juist uitvoeren van deze beleidsregel?
I	Wie moet geïnformeerd worden voor het juist uitvoeren van deze beleidsregel?

Versiebeheer

Versie	Status	Wijziging	Datum
1.1	Concept	Beleid Gegevensbescherming	20-08-2015
1.4	Concept	Volledig herzien van het privacybeleid	07-08-2018
1.5	Concept	Omvorming naar privacyhandboek bespreekstuk	05-10-2018
1.6	Concept	Verwerkingen n.a.v. eerste uitrol	24-10-2018
1.7	Concept	Alle input eerste uitrol verwerkt	2-11-2018
2.0	Definitief	Eerste definitieve versie	13-11-2018

Afkortingen

Afkorting	Omschrijving
AVG	Algemene Verordening Gegevensbescherming
IB&P	Informatiebeveiligings- en privacyteam
PbD	Privacy by Design
VSP	Virtueel Servicepunt
JZ	Juridische Zaken (Servicepunt71)
DIV	Documentaire Informatievoorziening

Begrippen

Begrip	Definitie
BETROKKENE	**De BETROKKENE is degene op wie het PERSOONSGEGEVEN betrekking heeft.** *Wettelijke definitie (AVG)* Een geïdentificeerde of identificeerbare natuurlijke persoon;
DOEL (DOELEINDE, VERWERKINGSDOEL, VERZAMELDOEL)	**Het DOEL waarvoor PERSOONSGEGEVENS worden verzameld of anderszins VERWERKT. Welke intentie heeft de VERANTWOORDELIJKE met deze VERWERKING van PERSOONSGEGEVENS? Welk doel wenst hij daarmee te bereiken?** *Wettelijke definitie (AVG)* Welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden[1].
GEMEENTE / SERVICEPUNT71	**Vul hier de eigen uitvoerende organisatie in. Vaak zullen dat de gemeenten Leiden, Leiderdorp, Oegstgeest, Zoeterwoude of Servicepunt71 zijn, maar het kan ook DZB, Erfgoed Leiden of De Lakenhal betreffen.**
PERSOONSGEGEVEN(S)	**Alle gegevens 'die iets zeggen' over een *natuurlijke* persoon (rechtspersonen als een besloten of naamloze vennootschap worden niet beschermd door de privacywetgeving).** Bijvoorbeeld: Naam, adres, woonplaats, e-mailadres, gebruikersnaam, bloedgroep, kenteken,

[1] PERSOONSGEGEVENS mogen slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde DOELEINDEN worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt;

	nationaliteit, IP-adres, postcode, geboortedatum, geslacht, geboorteplaats, mac-adres, salaris, etniciteit, IBAN, gezinssamenstelling, hoogte studieschuld, lengte, lichaamsgewicht, gezondheidsgegevens, lidmaatschappen, strafrechtelijke gegevens, seksuele voorkeur, BSN etc.
	Wettelijke definitie (AVG) Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de BETROKKENE"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
VERANTWOORDELIJKE (VERWERKINGS-VERANTWOORDELIJKE)	**Degene (persoon of organisatie) die het voor wat de VERWERKING betreft voor het zeggen heeft. De VERANTWOORDELIJKE bepaalt of er een VERWERKING van PERSOONSGEGEVENS plaatsvindt, welke PERSOONSGEGEVENS worden VERWERKT, waarom (voor welk DOEL), onder welke omstandigheden, op welke wijze enz. enz. De wet noemt dit 'bepalen van doel en middelen'.**
	Wettelijke definitie (AVG) Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die / dat, alleen of samen met anderen, het DOEL van en de middelen voor de VERWERKING van PERSOONSGEGEVENS vaststelt; wanneer de DOELSTELLINGEN van en de middelen voor deze VERWERKING in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de VERWERKINGSVERANTWOORDELIJKE is of volgens welke criteria deze wordt aangewezen.
VERWERKER	**De VERWERKER is degene die in opdracht van de (VERWERKINGS-) VERANTWOORDELIJKE PERSOONSGEGEVENS VERWERKT.**
	Wettelijke definitie (AVG) Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die / dat ten behoeve van de VERWERKINGSVERANTWOORDELIJKE PERSOONSGEGEVENS VERWERKT.
VERWERKING (VERWERKEN)	**Alles wat je doet met een of meer PERSOONSGEGEVENS, alsmede het geheel van samenhangende werkzaamheden.**
	Wettelijke definitie (AVG) Een VERWERKING of een geheel van VERWERKINGEN met betrekking tot PERSOONSGEGEVENS of een geheel van PERSOONSGEGEVENS, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

1. Algemene omgang met persoonsgegevens

Uitgangspunt

De Leidse Regio VERWERKT PERSOONSGEGEVENS slechts in overeenstemming met de AVG. Bij alle VERWERKINGEN die plaatsvinden worden de hieronder besproken beginselen in acht genomen.

Realisatie

- **Rechtmatigheid**

  PERSOONSGEGEVENS mogen slechts worden VERWERKT voor zover dit noodzakelijk is ten behoeve van één van de onderstaande DOELEINDEN (*rechtmatigheid*). Hieronder worden de 6 mogelijke verwerkingsgrondslagen toegelicht:

  1. *Toestemming:*

  De BETROKKENE moet in dit geval toestemming geven. De BETROKKENE moet goed geïnformeerd zijn, zich vrij voelen om de toestemming eventueel te weigeren en een duidelijke actieve handeling verrichten om toestemming te verlenen. De toestemming moet gaan over een specifieke GEGEVENSVERWERKING en, op vergelijkbare wijze als het verlenen van de toestemming, weer kunnen worden ingetrokken.

  Voorbeeld: Het aanmelden voor de gemeentelijke nieuwsbrief.

  2. *Overeenkomst:*

  Het gaat hier om de GEGEVENSVERWERKING noodzakelijk voor het afsluiten en nakomen van een overeenkomst, dit betreffen altijd de persoonsgegevens van de wederpartij.

  Voorbeeld: De verhuur van een sportaccommodatie inclusief contractuele afspraken en facturering.

  3. *Wettelijke verplichting:*

  De gegevensverwerking is noodzakelijk om aan een wettelijke verplichting te voldoen.

  Voorbeeld: Het vastleggen van gegevens in een dossier over de hulp of zorg die een burger in het kader van de Wmo heeft ontvangen (dossierplicht).

  4. *Vitale belangen:*

  De gegevensverwerking is essentieel voor iemands leven of gezondheid en je kunt die persoon niet om toestemming kunt vragen.

  Voorbeeld: Bij een grootschalige ramp moet er onmiddellijk hulp geboden kunnen worden.

  5. *Algemeen belang en openbaar gezag:*

  Het gaat hier om taken die in een wet zijn vastgelegd voor jouw organisatie, hier kan ook wel gesproken worden over het uitvoeren van de ‘publieke taak’.

  Voorbeeld: Gemeentelijk cameratoezicht in de openbare ruimte ten behoeve van de openbare veiligheid.

  6. *Gerechtvaardigd belang:*

  Het betreffen hier VERWERKINGEN die noodzakelijk zijn t.b.v. het gerechtvaardigd

bedrijfsbelang, dit belang moet worden afgewogen tegen het recht op privacy van de BETROKKENE.

Voorbeeld: Het voeren van een personeelsadministratie.

- **Behoorlijkheid, transparantie en doelbinding**
  Gegevensverwerking moet op een behoorlijke wijze plaatsvinden (*behoorlijkheid*) en het moet voor de BETROKKENE zo duidelijk mogelijk zijn wat er met zijn PERSOONSGEGEVENS gebeurt (*transparantie*). Op het moment dat PERSOONSGEGEVENS worden verzameld, moet de BETROKKENE worden geïnformeerd over het DOEL waarvoor de PERSOONSGEGEVENS worden verzameld. Dit DOEL moet welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn.[2] De verzamelde PERSOONSGEGEVENS mogen vervolgens ook alleen voor dit DOEL verwerkt worden, verder VERWERKEN voor andere DOELEINDEN is in beginsel niet toegestaan (*doelbinding*).

- **Dataminimalisatie, juistheid, opslagbeperking, integriteit & vertrouwelijkheid**
  PERSOONSGEGEVENS moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de DOELEINDEN waarvoor zij worden verwerkt (*dataminimalisatie*). Verder moeten PERSOONSGEGEVENS worden geactualiseerd. Onjuiste gegevens moeten worden gewist of gerectificeerd (*juistheid*). Als je PERSOONSGEGEVENS opslaat, mag je deze in beginsel niet langer bewaren dan noodzakelijk met het oog op het DOEL waarvoor ze worden VERWERKT (*opslagbeperking*). Tot slot moeten PERSOONSGEGEVENS goed beveiligd worden en vertrouwelijk worden behandeld (*integriteit* & *vertrouwelijkheid*).

- **Verantwoordingsplicht**
  De verantwoordingsplicht houdt in dat, wanneer je PERSOONSGEGEVENS VERWERKT, je steeds moet kunnen aantonen dat je dat in overeenstemming met de AVG doet. Dit is de reden dat de AVG relatief veel administratieverplichtingen bevat.

Instructies

- ✓ VERWERK PERSOONSGEGEVENS in overeenstemming met dit handboek en de onderwerp-specifieke werkwijzen en procedures waarnaar in dit handboek verwezen wordt.
- ✓ Bij twijfel of onduidelijkheid: consulteer de privacybeheerder van jouw organisatie:
  Gemeente Leiden: Rozemarijn Smink (r.smink@leiden.nl)
  Gemeente Leiderdorp: Anne-Marie Beens (a.beens@leiden.nl)
  Gemeente Oegstgeest: Savanne Hintzen (s.hintzen@leiden.nl)
  Gemeente Zoeterwoude: Rozemarijn Smink (r.smink@leiden.nl)
  Servicepunt71: Rudolf Kroes (r.kroes@leiden.nl)

[2] Dit betekent dat het doel duidelijk omkaderd moet zijn: het mag niet te breed omschreven zijn. Verder moet er een verwerkingsgrondslag zijn (bijv. toestemming, noodzakelijk ter uitvoering overeenkomst etc.)

Verantwoordelijkheden

[**R**]esponsible [**A**]ccountable [**C**]onsulted [**I**]nformed	
R	Medewerker die de PERSOONSGEGEVENS VERWERKT.
A	Afdelingshoofd/teammanager onder wiens verantwoordelijkheid de VERWERKING wordt uitgevoerd.
C	Privacybeheerder / Informatiebeveiliger / Functionaris Gegevensbescherming.
I	BETROKKENEN.

2. Nieuwe of gewijzigde verwerkingen

Uitgangspunt

Iedere nieuwe VERWERKING van PERSOONSGEGEVENS, of wijziging van een reeds bestaande VERWERKING van PERSOONSGEGEVENS (bv. nieuwe IT-systemen, samenwerkingsverbanden, gegevensuitwisselingen, etc.), wordt volgens de principes van Privacy by Design en Privacy by Default vormgegeven en voorafgegaan door een beoordeling van de privacyaspecten van de VERWERKING.

Realisatie

Voorafgaand aan iedere nieuwe VERWERKING van PERSOONSGEGEVENS of elke wijziging van een reeds bestaande VERWERKING van PERSOONSGEGEVENS (hierna te noemen: wijziging) wordt:

- **de verwerking conform de beginselen van Privacy by Design vormgegeven;** (**1**)
  De werkwijze 'Privacy by Design'[3] biedt concrete maatregelen die zoveel mogelijk doorgevoerd moeten worden in het ontwerp. Hiermee wordt gegarandeerd dat een ontwerp zo privacy-vriendelijk mogelijk is vormgegeven. Het toepassen van Privacy by Design (PbD) is wettelijk verplicht. Het toepassen van deze werkwijze is vroeg in de vormgeving van de GEGEVENSVERWERKING wenselijk, hierdoor kan worden voorkomen dat later zaken hersteld moeten worden. Gedurende het proces moet worden gedocumenteerd welke maatregelen zijn doorgevoerd, op welke wijze en welke overwegingen ten grondslag liggen aan het niet-doorvoeren van bepaalde maatregelen. Privacy by Default zijn de instellingen van een programma, app, website of dienst, zodanig ingeregeld dat maximale privacy wordt betracht.

- **een Baselinetoets uitgevoerd; (2)**
  Dit is een toets aan de hand waarvan het risico van de VERWERKING wordt bepaald (en gedocumenteerd). Hieruit volgt of er een verplichting bestaat tot het uitvoeren van een Privacy impact assessment (PIA) en / of een diepgaande risico analyse. Neem contact op met de privacybeheerder en / of informatiebeveiliger van jouw organisatie om de baselinetoets uit te voeren.

- **indien blijkt dat dit noodzakelijk is, een PIA en diepgaande risicoanalyse uitgevoerd; (3)**
  PIA's en diepgaande risico analyses zijn instrumenten met behulp waarvan, voorafgaand aan de daadwerkelijke GEGEVENSVERWERKING, de privacy risico's en benodigde informatiebeveiligingsmaatregelen in kaart worden gebracht, beoordeeld en waarin maatregelen worden voorgesteld om de eventuele negatieve gevolgen tot een minimum te beperken.

- **voorzien in de nodige contractuele afspraken;** (**4**)
  Indien er derden worden ingeschakeld voor de nieuwe VERWERKING van PERSOONSGEGEVENS volg je hoofdstuk zes ('*Inschakelen van derden*').

[3] Dit document is op dit moment nog niet beschikbaar. Wanneer dit Handboek definitief wordt gemaakt zullen alle documenten waar naar verwezen wordt gereed zijn, dit is naar verwachting Q1 2019.

- **het register van verwerkingen actueel gehouden; (5)**
  In het register van verwerkingen dient een actueel overzicht van alle VERWERKINGEN van PERSOONSGEGEVENS te staan. Neem contact op met de privacybeheerder van jouw organisatie om het register n.a.v. de nieuwe VERWERKING of wijziging te actualiseren.

De onder punt 2 en 3 genoemde toetsen worden met hulp van de privacybeheerder en / of informatiebeveiliger opgesteld en indien nodig voorgelegd aan de Functionaris Gegevensbescherming. De opgestelde documenten worden toegevoegd aan het projectdossier.

Gemeente Leiden: Rozemarijn Smink (r.smink@leiden.nl)
Gemeente Leiderdorp: Anne-Marie Beens (a.beens@leiden.nl)
Gemeente Oegstgeest: Savanne Hintzen (s.hintzen@leiden.nl)
Gemeente Zoeterwoude: Rozemarijn Smink (r.smink@leiden.nl)
Servicepunt71: Rudolf Kroes (r.kroes@leiden.nl)

Instructies

- ✓ (**1**) pas de werkwijze 'Privacy by Design'[4] toe bij het ontwerpen van nieuwe VERWERKINGEN en het wijzigen van bestaande VERWERKINGEN;
- ✓ (**2**) voer een Baselinetoets uit;
- ✓ (**3**) voer zo nodig een PIA en diepgaande risicoanalyse uit;
- ✓ (**4**) volg hoofdstuk zes ('*Inschakelen van derden*') indien er derden worden ingeschakeld.
- ✓ (**5**) actualiseer het register van verwerkingen

Verwijzing

- ☞ **Werkwijze 'Privacy by Design'[5]**
  Uitleg: De PbD-werkwijze schrijft concrete maatregelen voor die, wanneer deze worden toegepast, garanderen dat een VERWERKING zo 'privacy-vriendelijk' mogelijk is vormgegeven. De wijze waarop een maatregel wordt toegepast moet worden gedocumenteerd en de onmogelijkheid om een maatregel toe te passen moet worden beargumenteerd.

[4] Dit document is op dit moment nog niet beschikbaar. Wanneer dit Handboek definitief wordt gemaakt zullen alle documenten waar naar verwezen wordt gereed zijn, dit is naar verwachting Q1 2019.

[5] Dit document is op dit moment nog niet beschikbaar. Wanneer dit Handboek definitief wordt gemaakt zullen alle documenten waar naar verwezen wordt gereed zijn, dit is naar verwachting Q1 2019.

Verantwoordelijkheden

[**R**]esponsible [**A**]ccountable [**C**]onsulted [**I**]nformed	
R	Projectleider of medewerker die de nieuwe of gewijzigde VERWERKING organiseert.
A	Projectopdrachtgever / afdelingshoofd die / dat verantwoordelijk wordt voor de VERWERKING.
C	Baseline: privacybeheerder / informatiebeveiliger; PIA: privacybeheerder / Functionaris Gegevensbescherming; Diepgaande risico analyse: informatiebeveiliger.
I	Functionaris Gegevensbescherming (voor het geheel).

3. Doelbinding

Uitgangspunt

Er worden alleen PERSOONSGEGEVENS VERWERKT voor DOELEINDEN die verenigbaar zijn met de DOELEINDEN waarvoor de PERSOONSGEGEVENS zijn verkregen.

Realisatie

De PERSOONSGEGEVENS die de gemeente / Servicepunt71 VERWERKT, zijn verzameld of verkregen om VERWERKT te worden voor een specifiek VERWERKINGSDOEL. In gevallen waarin PERSOONSGEGEVENS voor een ander DOEL worden verwerkt dan waarvoor ze aanvankelijk zijn verzameld, moet worden beoordeeld of de DOELEN verenigbaar zijn.

Voorbeeld

Een BETROKKENE geeft zijn e-mailadres bij het aanvragen van zijn paspoort, hij wil graag geïnformeerd worden wanneer het paspoort opgehaald kan worden. De gemeente gebruikt dit PERSOONSGEGEVEN vervolgens om BETROKKENE uit te nodigen stembureaulid te worden bij de volgende verkiezingen. In dit geval worden de PERSOONSGEGEVENS voor een ander DOEL verder VERWERKT terwijl dit niet verenigbaar is.
Het uitsturen van een enquête over de kwaliteit van de baliedienst, zou in dit geval wel een verdere VERWERKING met verenigbaar DOEL zijn.

Een ander voorbeeld is het VERWERKEN van PERSOONSGEGEVENS voor TESTDOELEINDEN of het toegang verkrijgen tot iemand zijn persoonlijke mailbox of netwerkschijf. Hiervoor zijn aparte procedure opgesteld. Zie hiervoor: Procedure testdata[6] en (Privacy)reglement e-mail en internetgebruik. (1)

- **Verder verwerken (2)**
  Al het hergebruik of verder VERWERKEN van PERSOONSGEGEVENS, moet via het reguliere proces (zie hoofdstuk 2) tot stand komen. Bij de beoordeling van de vraag of de beoogde VERWERKING verenigbaar is met het DOEL waarvoor de PERSOONSGEGEVENS aanvankelijk zijn verzameld wordt onder meer rekening gehouden met:
  a. ieder verband tussen de DOELEINDEN waarvoor de persoonsgegevens zijn verzameld, en de DOELEINDEN van de voorgenomen (verdere) VERWERKING;
  b. het kader waarin de persoonsgegevens zijn verzameld, met name de verhouding tussen de BETROKKENEN en de VERWERKINGSVERANTWOORDELIJKE;
  c. de aard van de PERSOONSGEGEVENS, met name of bijzondere categorieën van PERSOONSGEGEVENS worden VERWERKT of PERSOONSGEGEVENS over strafrechtelijke veroordelingen en strafbare feiten;
  d. de mogelijke gevolgen van de voorgenomen verdere VERWERKING voor de BETROKKENEN;
  e. het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering van de PERSOONSGEGEVENS.

[6] Dit document is op dit moment nog niet beschikbaar. Wanneer dit Handboek definitief wordt gemaakt zullen alle documenten waar naar verwezen wordt gereed zijn, dit is naar verwachting Q1 2019.

Instructies

- ✓ (**1**) Volg eventueel aanwezige onderwerp-specifieke procedures of reglementen.
- ✓ (**2**) Volg in alle overige gevallen *hoofdstuk 2: Nieuwe of gewijzigde verwerkingen*.

Verwijzing

- ☞ **Procedure Testdata**
  Uitleg: Testen worden alleen uitgevoerd conform de procedure Testdata.[7] Toepassing van deze procedure moet een redelijke mate van zekerheid geven dat, ten aanzien van testen, de nodige waarborgen worden toegepast en afwegingen worden gemaakt.
  Vindplaats: VSP (link volgt)

- ☞ **(Privacy)reglement e-mail en internetgebruik**
  Uitleg: Reglementen over het gebruik van en de controle op het e-mail en internetgedrag van medewerkers.
  Vindplaats: http://virtueel.servicepunt71.nl/medewerker/themas/mijn-werkplek/informatiebeveiliging-privacy/privacyreglement-e-mail-en-internetgebruik/

- ☞ **Privacy beleid**
  Uitleg: De gemeentelijke visie op privacy en de kaders waarbinnen daarop gehandeld kan worden.[8]
  Vindplaats: VSP (link volgt)

Verantwoordelijkheden

[**R**]esponsible [**A**]ccountable [**C**]onsulted [**I**]nformed	
R	Medewerkers
A	Afdelingshoofden
C	Privacybeheerder (Via Baseline en PIA en op verzoek voor advies) en Informatiebeveiliger (Via Baseline en Diepgaande Risicoanalyse)
I	Privacybeheerder (m.b.t. het register van verwerkingen)

[7] Dit document is op dit moment nog niet beschikbaar. Wanneer dit Handboek definitief wordt gemaakt zullen alle documenten waar naar verwezen wordt gereed zijn, dit is naar verwachting Q1 2019.

[8] Dit document is op dit moment nog niet beschikbaar. Wanneer dit Handboek definitief wordt gemaakt zullen alle documenten waar naar verwezen wordt gereed zijn, dit is naar verwachting Q1 2019.

4. Beveiligingsincidenten en datalekken

Uitgangspunt

Meld een incident zo spoedig mogelijk na ontdekking en zorg dat de schade beperkt blijft. Raak niet in paniek en deel de gegevens voorlopig niet met nog meer mensen.

Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat informatie in gevaar is of kan komen. Er is sprake van een datalek als PERSOONSGEGEVENS betrokken zijn bij het beveiligingsincident.

Een beveiligingsincident of datalek (hierna samen te noemen: incident) wordt zo spoedig mogelijk na de melding daarvan beoordeeld. Blijkt het incident een datalek te zijn, dan kan de wet vereisen dat dit gemeld wordt bij de toezichthouder en eventueel de BETROKKENE(N).

Medewerkers zijn oplettend en melden een door hen opgemerkt incident, of een vermoeden daarvan, altijd bij het afdelingshoofd of de teammanager en iemand van het informatiebeveiligings- en privacyteam. Medewerkers moeten zich altijd vrij voelen een incident, of een vermoeden daarvan, te melden.

Realisatie

- **Intern melden van incident**
  Van medewerkers wordt verondersteld dat zij oplettend zijn en wanneer zij een incident opmerken / vermoeden, zij dit zo spoedig mogelijk melden.

- **Procedure datalekken**
  In geval een datalek zich voordoet, wordt dit door het informatiebeveiliging- en privacyteam (IB&P) afgehandeld conform de procedure Meldplicht Datalekken.[9]

Instructies

- ✓ **Heb je een incident opgemerkt? Meld het direct!**

  Telefonisch / e-mail: *Bij de informatiebeveiliging- en/of privacy contactpersoon van jouw organisatie of bij de Functionaris Gegevensbescherming.*

  Gemeente Leiden: Martin van Zuuk (IB) en Rozemarijn Smink (P)
  Gemeente Leiderdorp: Ab Errami (IB) en Anne-Marie Beens (P)
  Gemeente Oegstgeest: Ab Errami (IB) en Savanne Hintzen (P)
  Gemeente Zoeterwoude: Janet van der Ree (IB) en Rozemarijn Smink (P)
  Servicepunt71: Maurice Derogee (IB) en Rudolf Kroes (P)

[9] Dit document is op dit moment nog niet beschikbaar. Wanneer dit Handboek definitief wordt gemaakt zullen alle documenten waar naar verwezen wordt gereed zijn, dit is naar verwachting Q1 2019.

Functionaris Gegevensbescherming: Robert Haasnoot (r.haasnoot@servicepunt71.nl)

Algemeen via: gegevensbescherming@servicepunt71.nl

Webformulier: *Zie het webformulier in het tabblad 'BEVEILIGINGSINCIDENT / DATALEK' op de intranetpagina Informatiebeveiliging & privacy onder 'MIJN WERKPLEK'.*

Vermeld hierbij de volgende informatie:
1. Geef een samenvatting van het incident: wat is er gebeurd?
Vermeld hier ook de naam van het betrokken systeem en de naam van het proces / de verwerking.

2. Welke typen PERSOONSGEGEVENS zijn betrokken bij het incident?
Bijvoorbeeld: naam, adres, e-mailadres, IP-adres, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.

3. Van hoeveel personen zijn de PERSOONSGEGEVENS betrokken bij het incident?
Geef a.u.b. een minimum en maximum aantal personen als het exacte aantal niet bekend is.

4. Omschrijving groep personen om wiens gegevens het gaat.
Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van kwetsbare groepen personen, zoals kinderen.

5. Zijn de contactgegevens van de betrokken personen bekend?
Het kan zijn dat BETROKKENEN geïnformeerd moeten worden over het datalek, kunnen we deze personen in dat geval bereiken?

6. Wat is de oorzaak van het incident?
Heb je een idee hoe het incident heeft kunnen ontstaan?

7. Op welke datum of in welke periode heeft het incident plaats kunnen vinden?
Geef dit a.u.b. zo specifiek mogelijk aan.

8. Welke maatregelen stel je voor?

Verwijzing

☞ **Proces melden datalek en beveiligingsincident**
Uitleg: Bovenstaande wordt in meer detail uiteengezet in deze procedure.
http://virtueel.servicepunt71.nl/fileadmin/ict/Handleidingen/Nieuw_VSP/Beveiliging/Proces_melden_datalek_-_beveiligingsincident.pdf

☞ **Stappenplan voor probleemverantwoordelijke beveiligingsincident / datalek**
Uitleg: Dit document is een verkort naslagwerk van de bovenstaande procedure.
Vindplaats:
http://virtueel.servicepunt71.nl/fileadmin/ict/Handleidingen/Nieuw_VSP/Beveiliging/Verkort_stappenplan_beveiligingsincident.pdf

☞ **Meer weten over een (mogelijk) datalek?**

Uitleg: VSP-pagina met meer informatie over een (mogelijk) datalek.

Vindplaats: http://virtueel.servicepunt71.nl/medewerker/themas/mijn-werkplek/informatiebeveiliging-privacy/beveiligingsincident-datalek-melden/

Verantwoordelijkheden

[**R**]esponsible [**A**]ccountable [**C**]onsulted [**I**]nformed	
R	Medewerker die het incident ontdekt / vermoedt (voor intern melden)
A	Afdelingshoofd van het team waar het incident heeft plaatsgevonden (afhandelen proces melden datalek en beveiligingsincident)
C	Informatiebeveiliger / privacybeheerder
I	Functionaris Gegevensbescherming, Autoriteit Persoonsgegevens, BETROKKENE(N), directeur, gemeentesecretaris, collegeleden (laatste 5 afhankelijk van de ernst)

5. Beveiliging

Uitgangspunt

PERSOONSGEGEVENS worden beveiligd d.m.v. het nemen van passende technische en organisatorische maatregelen. Hierbij wordt rekening gehouden met de aard, omvang, context, DOELEINDEN en risico's van de VERWERKING.[10] Ook wanneer de gemeente / Servicepunt71 PERSOONSGEGEVENS door een VERWERKER laat VERWERKEN, wordt ervoor gezorgd dat de PERSOONSGEGEVENS voldoende worden beveiligd.

Realisatie

- Bij het initiëren van een nieuwe VERWERKING van PERSOONSGEGEVENS of wijzigen van een bestaande VERWERKING, worden passende (technisch & organisatorisch) beveiligingsmaatregelen getroffen conform het Informatiebeveiligingsbeleid.

Instructies

✓ Kies passende technische en organisatorische beveiligingsmaatregelen conform het Informatiebeveiligingsbeleid en pas deze toe.

Voorbeeld

Het versturen van PERSOONSGEGEVENS is een manier van het VERWERKEN van PERSOONSGEGEVENS. Het goed beveiligen is daarom ook hier van belang. Wanneer een reguliere e-mail wordt verzonden kan dit worden gezien als het versturen van een postkaart qua beveiligingsniveau, erg onveilig dus.

Het veilig verzenden van e-mail kan via:

- ENCRYPT typen in de onderwerp-regel van je e-mail (alleen te gebruiken bij externe mailadressen). Bijvoorbeeld: 'ENCRYPT Verzoek om informatie'. Wanneer je dit doet ontvang jij een wachtwoord dat je aan de ontvangende partij kunt doorbellen, deze kan daarmee het bericht downloaden.
- Om ook intern beveiligd te mailen kun je e-mails verzenden via ZIVVER.[11]

Verwijzing

☞ **Informatiebeveiligingsbeleid**
Uitleg: Beleidsstuk waarin de wijze waarop de gemeente / Servicepunt71 omgaat met de beveiliging van informatie is beschreven.

Vindplaats: http://virtueel.servicepunt71.nl/nc/medewerker/themas/mijn-werkplek/informatiebeveiliging-privacy/informatie-beveiligen/

[10] Zie ook hoofdstuk 2.

[11] Op dit moment is ZIVVER helaas nog niet geïmplementeerd voor de hele regio, houdt de intranetpagina in de gaten voor de actuele stand van zaken hieromtrent.

☞ **Veilig mobiel werken**

Uitleg: Intranetpagina met informatie voor jou over veilig mobiel werken, met je eigen apparaat of mobiel apparaat wat je van je werkgever in bruikleen hebt.

Vindplaats: http://virtueel.servicepunt71.nl/medewerker/themas/mijn-werkplek/informatiebeveiliging-privacy/veilig-mobiel-werken/

☞ **Zo maak je een sterk wachtwoord**

Uitleg: Internetpagina met informatie voor jou over het instellen en onthouden van een sterk wachtwoord.

Vindplaats: https://toolbox.bof.nl/adviezen/wachtwoord/

Verantwoordelijkheden

[**R**]esponsible[**A**]ccountable [**C**]onsulted [**I**]nformed	
R	Uitvoerend medewerker
A	Verantwoordelijk afdelingshoofd
C	Informatiebeveiliger
I	Privacybeheerder / Functionaris Gegevensbescherming

6. Inschakelen van en doorgifte aan derden

Uitgangspunt

De gemeente / Servicepunt71 kan persoonsgegevens doorgeven / uitwisselen met derden, op basis van verschillende relaties. Elke doorgifte / uitwisseling moet voldoen aan de eisen van de AVG en aan een passend niveau van informatiebeveiliging. Hierover worden afspraken gemaakt in overeenkomsten, welke overeenkomst nodig is is afhankelijk van het type relatie.

Verwerkers (verantwoordelijke-verwerker relatie)

De gemeente / Servicepunt71 (verantwoordelijke) schakelt een derde (verwerker) in, met als belangrijkste doel het verwerken van persoonsgegevens. De verantwoordelijke bepaalt hierbij het doel en middelen, de verwerker volgt slechts instructies op. Met een verwerker worden afspraken gemaakt in een verwerkersovereenkomst.

> **Voorbeeld**
>
> Een voorbeeld van een verantwoordelijke-verwerker relatie is een salarisadministratiekantoor. Er is hier sprake van een verwerker omdat de opdracht zich primair richt op het verwerken van persoonsgegevens. Een ander voorbeeld een applicatie die in de cloud staat.

Gezamenlijke (verwerkings)verantwoordelijkheid

Wanneer de gemeente / Servicepunt71 het doel en de middelen van de verwerking in samenspraak met een derde bepaalt, is er sprake van gezamenlijke- of medeverantwoordelijkheid. Dit is het geval als er een uitwisseling van persoonsgegevens voortvloeit uit afspraken die partijen op gelijkwaardige voet met elkaar gemaakt hebben. Bij deze relatie moet er een gezamenlijke verantwoordelijkheidsovereenkomst afgesloten worden.

> **Voorbeeld**
>
> Een voorbeeld van een (mede)verwerkingsverantwoordelijke is een zorgorganisatie die op grond van de Wet maatschappelijke ondersteuning (Wmo) in opdracht van de gemeente huishoudelijke hulp verleent. Deze zorgorganisatie verwerkt bij die zorgverlening gegevens van de cliënten.
>
> Het verlenen van de huishoudelijke zorg is de primaire taak, het verwerken van de persoonsgegevens vloeit hieruit voort. De zorgorganisatie is daarom geen verwerker maar medeverwerkingsverantwoordelijke.

Ontvangers (verantwoordelijke-verantwoordelijke relatie)

De gemeente / Servicepunt71 (verantwoordelijke) kan persoonsgegevens doorgeven aan een derde (verantwoordelijke), die vervolgens zelfstandig over

het doel en de middelen beslist. Dit vindt alleen plaats als er een verplichting of een sterke, rechtmatige reden daartoe bestaat. Dit laatste dient goed getoetst te worden.

> **Voorbeeld**
>
> Het als werkgever verstrekken van persoonsgegevens aan de Belastingdienst in het kader van de loonheffing. Voor het delen van deze gegevens hoeft geen overeenkomst afgesloten te worden, wel moet gewaarborgd worden dat de gegevensuitwisseling passend beveiligd wordt.

Realisatie

- **Vaststellen rolverdeling**
  Indien er derden betrokken zijn bij het VERWERKEN van PERSOONSGEGEVENS: stel vast wat de AVG-rollen van de betrokken partijen zijn .

- **Verwerkersovereenkomst (in geval VERANTWOORDELIJKE-VERWERKER-relatie)**
  Is er sprake van een VERANTWOORDELIJKE-VERWERKER-relatie? Dan draagt het afdelingshoofd er zorg toe dat er voorafgaand aan de GEGEVENSVERWERKING een verwerkersovereenkomst gesloten wordt met de beoogde VERWERKER.

- **Gezamenlijke verantwoordelijkheidsovereenkomst (in geval gezamenlijke verantwoordelijkheid)**
  Wanneer de gemeente / Servicepunt71 samen met een derde het DOEL en de middelen van een VERWERKING van PERSOONSGEGEVENS bepaalt, maken deze partijen afspraken hierover in een gezamenlijke VERWERKINGSVERANTWOORDELIJKE overeenkomst.

- **Onderzoek rechtmatigheid en waarborgen (in geval verantwoordelijke-verantwoordelijke-relatie)**
  Wanneer een derde PERSOONSGEGEVENS ontvangt die deze derde op eigen VERANTWOORDELIJKHEID verder VERWERKT, hoeft de gemeente / Servicepunt71 hierover in beginsel geen afspraken te maken. Van groot belang is dat de doorgifte (zelf een VERWERKING) wel is toegestaan. Ook dient een passende beveiligingsniveau voor de beoogde gegevensuitwisseling gewaarborgd te zijn.

Het informatiebeveiligings- en privacyteam en / of Juridische Zaken (JZ) kunnen inhoudelijke ondersteuning bieden bij de bovenstaande realisaties.

Instructies

- ✓ Stel vast wat de AVG-rol is van de gemeente / Servicepunt71 en de derde(n);
- ✓ Beoordeel de rechtmatigheid van de verstrekking van PERSOONSGEGEVENS aan de ontvanger. Beoordeel eveneens of de voorgenomen waarborgen voldoende zijn. Dit kan met behulp van de baselinetoets;
- ✓ Sluit – indien van toepassing – een verwerkersovereenkomst of een gezamenlijke VERWERKINGSVERANTWOORDELIJKE overeenkomst;
- ✓ De ondertekende overeenkomsten worden bij contactbeheer aanleveren via contracten@servicepunt71.nl;
- ✓ Actualiseer het register van verwerkingen door deze gegevensuitwisseling toe te voegen.

Verwijzing

☞ **Verwerkersovereenkomst**

Uitleg: Overeenkomst voor verantwoordelijke-verwerker relatie.

Vindplaats: Een standaard versie is op te vragen bij de privacybeheerder, binnenkort zal deze ook via het VSP beschikbaar worden.

☞ **Gezamenlijke verantwoordelijkheidsovereenkomst**

Uitleg: Overeenkomst voor gezamenlijke verantwoordelijke relatie.

Vindplaats: Een standaard versie is op te vragen bij de privacybeheerder, binnenkort zal deze ook via het VSP beschikbaar worden.

☞ **Stroomschema overeenkomsten uitwisseling persoonsgegevens**

Uitleg: Een stroomschema dat helpt in te schatten wat voor soort overeenkomst er welke situatie afgesloten moet worden.

Vindplaats: Op de Privacypagina van het VSP

Verantwoordelijkheden

[**R**]esponsible[**A**]ccountable [**C**]onsulted [**I**]nformed	
R	Uitvoerende medewerker
A	Verantwoordelijk afdelingshoofd
C	Informatiebeveiliger / Privacybeheerder / Juridische Zaken
I	Contractbeheer / Inkoop

7. Archiveren en vernietigen

Uitgangspunt

De gemeente / Servicepunt71 bewaart PERSOONSGEGEVENS slechts (in een tot personen herleidbare vorm) zo lang als noodzakelijk is voor het DOEL waarvoor deze gegevens VERWERKT worden en om te voldoen aan een wettelijke verplichting zoals bijvoorbeeld vastgelegd in de Archiefwet. Het is niet toegestaan om documenten langer of korter te bewaren dan is vastgelegd.

Realisatie

Bewaartermijnen t.b.v. archivering

- Er is op grond van de AVG geen concrete bewaartermijn voor PERSOONSGEGEVENS. Wel zijn er concrete bewaartermijnen in andere wetten waar overheden zich aan moeten houden. Doorgaans hebben de meeste processen (en de documenten die daaruit voortvloeien) bij de gemeente al een vastgestelde bewaartermijn. Hanteer deze bewaartermijn zorgvuldig. (1)

Voorbeeld

Een voorbeeld van documenten met een duidelijke maximale bewaartermijn zijn cv's en sollicitatiebrieven. Hierbij wordt onderscheid gemaakt tussen een gerichte sollicitatie en een open sollicitatie.

Gerichte sollicitatie: maximaal vier weken bewaren, daarna vernietigen. Dat geldt dus ook voor alle collega's die deze sollicitatie ter beoordeling of als bijwoners van het gesprek ontvangen hebben!
Open sollicitatie: maximaal één jaar bewaren, maar alleen als de sollicitant daar expliciet toestemming voor heeft gegeven.

- Geen bewaartermijn vastgesteld? De 'Selectielijst gemeenten en intergemeentelijke organen' is leidend bij de gemeente in het bepalen van een bewaartermijn t.b.v. archivering. Betrek de afdeling DIV / Documenten bij het maken van een keuze. (2)

- In principe is de afdeling DIV / Documenten verantwoordelijk voor de naleving van bewaartermijnen, in samenwerking met de 'producenten' van de documenten. Zorg dat bewaartermijnen structureel worden opgevolgd. Gebruik hier bijvoorbeeld de Richtlijnen voor vernietigen voor. (3)

- Eventuele VERWERKERS zijn ook aan bewaartermijnen gebonden. Bij samenwerkingsverbanden, dus als er (sub)VERWERKERS ingeschakeld zijn, moeten bewaartermijnen voor deze partij via de verwerkersovereenkomst vastgelegd worden. (4)

Registratie

- Archiveer informatie op de juiste wijze in een archief(systeem), zodat het beheerd kan worden. Alle vormen van informatie kunnen archiefwaardig zijn (dus e-mails, brieven, bierviltjes etc.) Verwijder de informatie uit niet-archief systemen/mappen/outlook en voorkom (al dan niet gestructureerde) schaduwarchieven. (5)

Voorbeeld

Het belang van goed archiveren werd pijnlijk duidelijk in de 'bonnetjesaffaire' van toenmalig staatssecretaris Teeven, oftewel de 'Teevendeal'.

De Teevendeal was een deels geheime schikking uit 2000–2001 tussen het Nederlandse Openbaar Ministerie (OM) en de drugshandelaar Cees H. Als onderdeel van deze schikking werd een eerder in beslag genomen bedrag van 4,7 miljoen gulden aan H. terugbetaald. De details van de schikking werden buiten het zicht van de Belastingdienst en de FIOD gehouden. Pas in 2014 kwam de deal opnieuw in de belangstelling door een uitzending van Nieuwsuur. Concreet bewijs (het 'bonnetje' van de transactie) ontbrak aanvankelijk, waardoor discussie ontstond over het precieze bedrag. Teeven zei zich het bedrag niet te herinneren. Pas in maart 2015 werd door het Ministerie van Veiligheid en Justitie alsnog het 'bonnetje' geleverd: uit een afschrift uit een verouderd financieel computersysteem bleek het werkelijke bedrag 4,7 miljoen gulden te zijn. Dat bonnetje had natuurlijk zonder moeite uit een geordend archief gehaald moeten worden…
Kort na het naar buiten komen van alle details trad Kamervoorzitter Van Miltenburg af, omdat zij eerder in het jaar een anonieme brief aan de Kamer met details over de Teevendeal had vernietigd. Ook vernietigen is immers aan strenge regels gebonden!

Instructies

- ✓ (**1**) Achterhaal de bewaartermijn(en) die bij jouw werkzaamheden van belang zijn;
- ✓ (**2**) Bepaal een bewaartermijn t.b.v. archivering op basis van de 'Selectielijst gemeenten en intergemeentelijke organanen'. Overleg deze keuze altijd met afdeling DIV / Documenten;
- ✓ (**3**) Pas deze termijnen structureel toe, eventueel met behulp van de Richtlijnen voor vernietigen;
- ✓ (**4**) Schrijf bewaartermijnen via verwerkersovereenkomst voor aan eventuele (sub)VERWERKERS;
- ✓ (**5**) Registreer informatie in een archief(systeem) en verwijder van overige opslagplaatsen. Bepaal of het archiefwaardig is m.b.v. opruimhulp.

Verwijzing

- ☞ **Selectielijst gemeenten en intergemeentelijke organen**
  Uitleg: Hierin staat beschreven wat de maximale en / of minimale termijn is dat data bewaard mag of moet worden door de gemeente / Servicepunt71.
  Vindplaats: https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/archieven/nieuws/selectielijst-gemeenten-en-intergemeentelijke-organen-2017

☞ **Richtlijnen voor vernietigen**

Uitleg: Hierin staat een stapsgewijze instructie voor het vernietigen van archiefstukken voor de gemeente Leiden beschreven.

Vindplaats:https://www.erfgoedleiden.nl/archiefzorg/overheidsarchieven/vernietiging

☞ **Opruimhulp**

Uitleg: Hierin staat beschreven wat informatie is om te archiveren en hoe je het beste het papieren archief kunt opruimen met daarbij een handige beslisboom

Vindplaats: PDF – Wat moet in archief? (volgt via intranet)

Verantwoordelijkheden

[**R**]esponsible [**A**]ccountable [**C**]onsulted [**I**]nformed	
R	Medewerkers zelf, afdeling DIV / team Documenten
A	Afdelingshoofd van het betreffende team, afdeling DIV / team Documenten
C	Afdeling DIV / team documenten, privacybeheerder
I	Afdeling DIV / team documenten, privacybeheerder

8. Bewustzijn

Uitgangspunt

Het beleid kan alleen worden uitgevoerd indien de medewerkers die het moeten toepassen op de hoogte zijn van de inhoud en concreet weten hoe te handelen. Daarom is het uitgangspunt dat alle medewerkers van de gemeente / Servicepunt71 op de hoogte zijn van het geldende privacybeleid. Dit handboek draagt bij aan het bewustzijn rondom het privacybeleid en zorgt voor het nemen van de juiste stappen.

Realisatie

De gemeente / Servicepunt71 verzorgt diverse activiteiten en neemt maatregelen om:

- het privacybeleid kenbaar te maken aan haar medewerkers;
- medewerkers in staat te stellen de nodige (basis)kennis gegevensbescherming te verkrijgen;
- medewerkers in staat te stellen VERWERKINGEN zelf in overeenstemming met de AVG te brengen.

Dit wordt bewerkstelligd door:

✓ **Goed inwerken**
Nieuwe medewerkers van de gemeente / Servicepunt71 worden spoedig na hun eerste werkdag gewezen op het privacybeleid en de onderliggende handboeken, werkwijzen en procedures.

✓ **Gegevensbescherming op het Virtueel Servicepunt (VSP)**
Op het VSP kunnen medewerkers informatie vinden die zij nodig hebben om hun werkzaamheden zelfstandig in lijn te brengen met de AVG.

✓ **E-learning**
De gemeente / Servicepunt71 zal op den duur aansluiten op een e-learning programma waarmee medewerkers hun kennis op het gebied van privacy en informatiebeveiliging kunnen vergroten;

✓ **Diverse trainingen, cursussen en activiteiten**
Het informatiebeveiligings- en privacyteam organiseert, al dan niet op aanvraag, diverse trainingen, cursussen en activiteiten op het gebied van informatiebeveiliging en privacy. Voorbeelden hiervan zijn de crisisgame, afdeling-specifieke trainingen, bewustwordingscampagnes, bezoeken aan werkoverleggen etc.

Verwijzing

☞ **Gegevensbescherming op het Virtueel Servicepunt**
Uitleg: Op het VSP kan de medewerker de nodige informatie vinden over gegevensbescherming.

Vindplaats: http://virtueel.servicepunt71.nl/medewerker/themas/mijn-werkplek/informatiebeveiliging-privacy/privacy-beschermen-avg/

☞ **Informatie en trainingen**

Vindplaats: VSP (Link volgt)

☞ **6 Gouden Regels**

Uitleg: Gebruik deze 6 Gouden Regels om je dagelijkse werkzaamheden zo (be)veilig(d) mogelijk uit te voeren.

Vindplaats: http://virtueel.servicepunt71.nl/nc/medewerker/themas/mijn-werkplek/informatiebeveiliging-privacy/informatie-beveiligen/

Verantwoordelijkheden

[**R**]esponsible [**A**]ccountable [**C**]onsulted [I]nformed	
R	Afdelingshoofd, Functionaris Gegevensbescherming
A	Medewerker zelf
C	VSP-pagina, privacybeheerder, informatiebeveiliger, beleidstukken en privacyhandboek
I	Collega's (kennisdeling)

9. Rechten van betrokkenen

Uitgangspunt

Iedere BETROKKENE (dit kan zowel een burger als een medewerker van de gemeente / Servicepunt71 zijn) heeft op grond van de AVG rechten die hij kan uitoefenen. Als een BETROKKENE één of meer van deze rechten inroept zijn wij, als gemeente / Servicepunt71 verplicht hier zo goed mogelijk gevolg aan te geven.

In de kern wil de AVG BETROKKENEN in staat stellen 'in control' te zijn over hun eigen PERSOONSGEGEVENS. Zij hebben met de komst van de AVG meer en uitgebreidere rechten toegekend gekregen met betrekking tot hun PERSOONSGEGEVENS en de VERWERKING daarvan.
BETROKKENEN hebben onder de AVG de volgende rechten:

- Recht van inzage;
- Recht op rectificatie;
- Recht op vergetelheid;
- Recht op beperking van de VERWERKING;
- Recht op dataportabiliteit (overdraagbaarheid GEGEVENS);
- Recht van bezwaar tegen VERWERKING;
- Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming / profiling.

De rechten die voor dit handboek van belang zijn, zijn het *recht van inzage* en het *recht op vergetelheid*. Dit hoofdstuk zal dan ook enkel toezien op deze twee rechten. Mocht je geïnteresseerd zijn in meer informatie over de andere rechten dan kan je de site van de Autoriteit Persoonsgegevens raadplegen. [12]

Recht van inzage
Een BETROKKENE kan met het recht op inzage achterhalen of en zo ja, welke PERSOONSGEGEVENS van hem of haar worden VERWERKT worden door de gemeente / Servicepunt71. De BETROKKENE kan een overzicht of kopie van de desbetreffende PERSOONSGEGEVENS opvragen. Ook de GEGEVENS die zich bevinden bij VERWERKERS of samenwerkingspartners kunnen onderdeel uitmaken van een dergelijk verzoek.

Recht op vergetelheid
Als men het heeft over het recht op vergetelheid wordt er ook wel van het recht op gegevenswissing gesproken, deze term spreekt iets meer tot de verbeelding.

[12] Voor verdere toelichting op de verschillende rechten kan de website van de autoriteit persoonsgegevens geraadpleegd worden. www.autoriteitpersoonsgegevens.nl.

Als de betrokkene een vergetelheidsverzoek indient bij onze gemeente / Servicepunt71 zullen we de PERSOONSGEGEVENS die we van de betrokkene VERWERKEN moeten wissen, indien dit mogelijk is. Wanneer de GEGEVENS worden verwerkt t.b.v. een rechtmatige GRONDSLAG, bijvoorbeeld de archiefwet, moet een vergetelheidverzoek worden afgewezen.

Termijnen
De termijn voor het afhandelen van 'rechten van BETROKKENE verzoeken' betreft één maand na ontvangst van het verzoek. Deze termijn kan wanneer dit noodzakelijk is worden verlengd met nog eens twee maanden. Het is van belang verzoeken van BETROKKENEN binnen deze termijn af te handelen. Ten eerste omdat de BETROKKENE hiermee zicht krijgt op het gebruik van zijn PERSOONSGEGEVENS en via deze rechten grip krijgt op zijn PERSOONSGEGEVENS. Maar ook omdat, wanneer de termijn verstrijkt, BETROKKENE een ingebrekestelling kan indienen en daarna, bij het uitblijven van een besluit, binnen twee weken een dwangsom kan vorderen. De Autoriteit Persoonsgegevens (hierna: AP), toezichthouder voor de AVG, kan daarnaast ook een dwangsom opleggen.[13]

Realisatie

Voor het goed kunnen afhandelen van het inzageverzoek dan wel het vergetelheidsverzoek is het belangrijk dat:

- het binnengekomen verzoek zo spoedig mogelijk wordt doorgezonden aan de privacybeheerder van jouw gemeente / Servicepunt71. (Het kan gebeuren dat het verzoek om de één of andere reden niet direct op de juiste plek terecht komt).
- zodra de privacybeheerder met een uitzoekvraag bij jou komt, jij dit zo spoedig mogelijk behandelt. Een desbetreffend verzoek heeft – in beginsel – voorrang op overig werk.
- als jij niet de aangewezen persoon bent voor de behandeling van het verzoek, je dit zo spoedig mogelijk laat weten aan de privacybeheerder. Indien voor jou bekend, met naam van de collega die wel de juiste persoon is.

Instructies

- ✓ Geef voorrang aan verzoeken (m.b.t. tot inzage- en vergetelheidsverzoeken) afkomstig van de privacybeheerder, vanwege de wettelijke beantwoordingstermijn van een maand vanuit de AVG.
- ✓ Bij twijfel of onduidelijkheid: consulteer de privacybeheerder van jouw organisatie:
  Gemeente Leiden: Rozemarijn Smink (r.smink@leiden.nl)
  Gemeente Leiderdorp: Anne-Marie Beens (a.beens@leiden.nl)
  Gemeente Oegstgeest: Savanne Hintzen (s.hintzen@leiden.nl)
  Gemeente Zoeterwoude: Rozemarijn Smink (r.smink@leiden.nl)
  Servicepunt71: Rudolf Kroes (r.kroes@leiden.nl)

[13] In 2017 heeft de AP een dwangsom van 46.000 ingevorderd voor het 4 weken te laat beantwoorden van een inzageverzoek (12.000 euro per week).

Verwijzing

☞ ***Procedure afhandeling inzageverzoek***
Uitleg: In deze procedure is stapsgewijs opgenomen hoe de privacybeheerder te werk gaat bij het afhandelen van het inzageverzoek. Er valt te lezen welke collega's op welk moment benaderd moeten worden voor het verzamelen van de relevante PERSOONSGEGEVENS. Daarnaast zijn er standaard brieven / documenten opgenomen die door iedere privacybeheerder worden gebruikt als basis om uniformiteit te waarborgen.

Vindplaats: VSP (Link volgt)

☞ ***Procedure afhandeling vergetelheidsverzoek***
Uitleg: In deze procedure is stapsgewijs opgenomen hoe de privacybeheerder te werk gaat bij het afhandelen van het vergetelheidsverzoek. Eerst zal moeten worden achterhaald welke GEGEVENS de gemeente / Servicepunt71 van de desbetreffende BETROKKENEN heeft, het eerste gedeelte van deze procedure zal dus sterk overeenkomen met die van het inzageverzoek. Daarnaast zal een goed overzicht te vinden zijn van de bewaartermijnen die gelden voor de verschillende GEGEVENS. Verder is opgenomen hoe en door wie de GEGEVENS feitelijk verwijderd zullen worden.

Vindplaats: VSP (Link volgt)

Verantwoordelijkheden

[**R**]esponsible[**A**]ccountable [**C**]onsulted [I]nformed	
R	Privacybeheerder (regie), teamleden van het team waar de GEGEVENS zich bevinden (GEGEVENS achterhalen / verwijderen)
A	Afdelingshoofd(en) van het(/de) team(s) waar de gegevens zich bevinden
C	Privacybeheerder, Afdeling DIV / Team Documenten, Functionaris Gegevensbescherming
I	BETROKKENE, Functionaris Gegevensbescherming