PRIVACY BY DESIGN AND DEFAULT

Procedure, checklist en werkblad

Juni 2019

Bron
Dyade

Bewerkt door:
Ronald van Rooijen

Versie	Status	Datum	Auteur	Omschrijving
0.1	Concept	24-01-2019	Dyade	Model
0.2	Concept	22-05-2019	JTC / CVW, RVO	Concept voor directie
	Vastgesteld			
	Gewijzigd			

Inleiding

In de Algemene verordening gegevensbescherming (AVG) is in artikel 25 geregeld dat verwerkingsverantwoordelijken invulling moeten geven aan gegevensbescherming door ontwerp en door standaardinstellingen. In de praktijk veelal aangeduid met de Engelse begrippen **Privacy by design** en **Privacy by default**. Hoewel privacy by design vooralsnog vooral een principiële set van algemene theoretische uitgangspunten is, zonder duidelijkheid over de precieze toepassing in de praktijk, is voorzien dat het wel een belangrijke rol zal spelen bij beoordeling van de rechtmatigheid van een verwerking door bijvoorbeeld de Autoriteit Persoonsgegevens (hierna AP).
Wat privacy by design dan inhoudt en hoe Stichting SOVOR / Jan Tinbergencollege daaraan invulling kan geven, staat in deze procedure, met een checklijst en een werkblad om de checklist in te vullen.

Wat zegt de AVG?

Artikel 25: Gegevensbescherming door ontwerp en door standaardinstellingen

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen.

2. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

3. Een overeenkomstig artikel 42 goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat aan de voorschriften van de leden 1 en 2 van dit artikel is voldaan.

Terminologie

Privacy by design houdt in dat organisaties al vanaf het begin van het ontwerpproces bij de ontwikkeling van nieuwe producten of diensten aandacht besteden aan technische en organisatorische privacyverhogende maatregelen en die inbouwen in processen en systemen.

De AVG onderscheidt twee doeleinden:

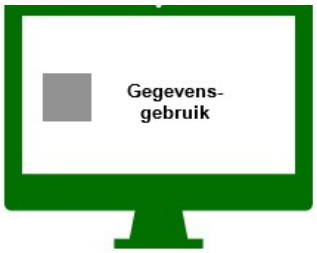
1. Waarborgen van de uitgangspunten van rechtmatige gegevensverwerking, met een focus op dataminimalisatie en pseudonimisering.
2. Inbouwen van de nodige waarborgen in de verwerking ter naleving van de AVG en in het bijzonder alle rechten van betrokkenen.

Rechtmatige gegevensverwerking is alleen gewaarborgd als aan een van de voorwaarden(grondslagen) is voldaan zoals opgenomen in artikel 6 van de AVG. Voor elke activiteit waarbij persoonsgegevens worden verwerkt, dient die grondslag te worden vastgelegd in het verplichte verwerkingsregister. De grondslagen zijn opgenomen in het werkblad van deze procedure.
Dataminimalisatie wil zeggen dat niet meer persoonsgegevens worden verwerkt dan strikt noodzakelijk is voor het doel van de verwerking.
Pseudonimisering is het versleutelen van gegevens op een zodanige manier dat de betrokkene niet meer rechtstreeks identificeerbaar is, maar wel individualiseerbaar. Dat gaat minder ver dan volledig anonimiseren, dus de AVG blijft wel van toepassing.
Anonimisering is het verwijderen van alle identificerende kenmerken van gegevens en van mogelijk indirect identificerende combinaties van gegevens. Is identificatie met voldoende zekerheid uitgesloten, dan zijn het geen persoonsgegevens meer en is de AVG niet van toepassing (wel op het anonimiseringsproces zelf).
Rechten van betrokkenen staan in artikel 13 t/m artikel 22 van de AVG en zijn als volgt samen te vatten:

Privacy by default is het principe dat de standaardinstellingen van elke dienst en elk product zo privacy vriendelijk mogelijk ingesteld moet zijn. Dat geldt (ook) voor bestaande diensten en producten.
Belangrijkste doelstelling is voorkomen dat persoonsgegevens onnodig openbaar worden, waarbij gebruikers niet hoeven op te letten dat zij onbewust toestemming geven om hun persoonsgegevens te verzamelen of te gebruiken voor niet noodzakelijke doeleinden.
Overigens moeten ook algemene voorwaarden privacy vriendelijk zijn geschreven, zonder verstopte privacy onderwerpen op een plaats waar ze niet thuishoren.

Voorbeelden

- Een goed voorbeeld van privacy by design is een systeem dat gegevens automatisch verwijdert op het moment dat de bewaartermijn verstrijkt.
- Een voorbeeld bij dataminimalisatie is dat bij de inrichting van een online-bestelproces het opvragen van een geboortedatum hoogstwaarschijnlijk niet noodzakelijk is, terwijl daarvoor in het verleden automatisch een invulveld werd ingericht. Vraag je wel naar die geboortedatum voor bijvoorbeeld marketingdoeleinden, dan mag het geen verplicht veld zijn en moet duidelijk zijn wat je ermee doet wanneer iemand het invult (transparantie).
- Bij privacy by default kan je een vergelijk maken met nieuwsbrieven waar voorheen het vinkje om je daarvoor aan te melden standaard al aanstond en je tegenwoordig zelf het vinkje moet aanzetten (actief dus) om de nieuwsbrief te kunnen ontvangen.
- Ander voorbeeld van privacy by default is dat een bezoeker van een website zelf moet kunnen bepalen welke cookies hij accepteert. Alleen het vinkje voor de (noodzakelijke) functionele cookies mag al van tevoren aanstaan. Verder kan je denken aan invulvelden op website-formulieren, het inloggen bij portals en gegevens die je opvraagt voor gebruikersaccountants.

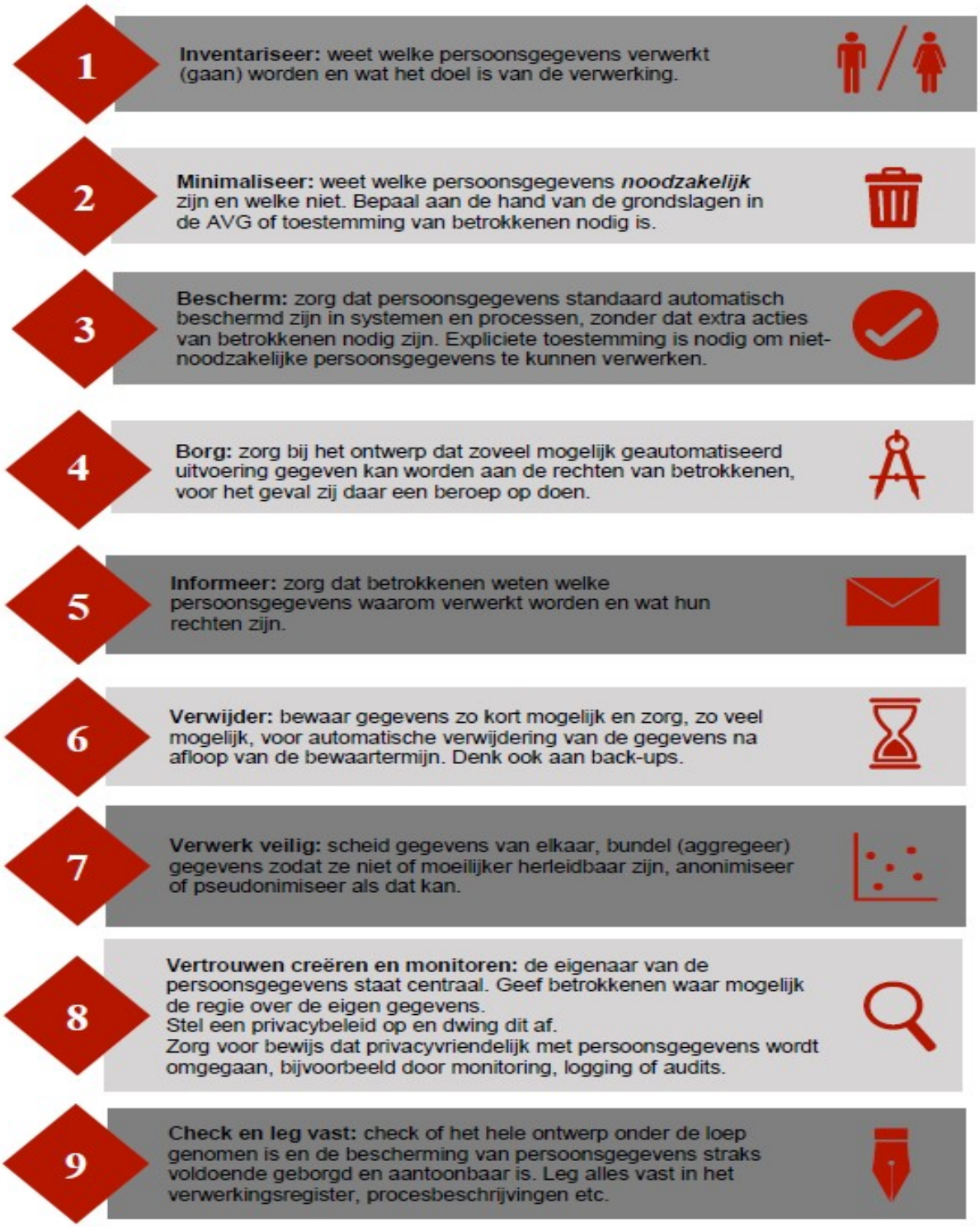


PRIVACY BY DESIGN & DEFAULT: UITGANGSPUNTEN

Privacy by design (waarin begrepen privacy by default) is gebaseerd op de volgende principes:

Privacy by design & default: checklist

Hoe kunnen we voldoen aan de principes van Privacy by design (waarin begrepen Privacy by default)?



PRIVACY BY DESIGN & DEFAULT: WERKBLAD

Werkblad voor het voldoen aan de principes van Privacy by design en default *		
	Checkpunt	**Uitwerking**
1.	**Inventariseer** • Welke persoonsgegevens verwerk je? • Wat is het doel daarvan?	
2.	**Minimaliseer** • Welke persoonsgegevens zijn noodzakelijk en welke niet? • Is op basis van de grondslagen in art. 6 AVG toestemming van betrokkenen nodig?	
3.	**Bescherm** Hoe zorg je ervoor dat persoonsgegevens standaard automatisch beschermd zijn in systemen en processen zonder dat extra acties van betrokkenen nodig zijn? Expliciete toestemming is nodig om niet-noodzakelijke persoonsgegevens te verwerken!	
4.	**Borg** Hoe zorg je ervoor dat bij het ontwerp zoveel mogelijk geautomatiseerd uitvoering gegeven kan worden aan de rechten van betrokkenen (art. 12 t/m 22 AVG) voor het geval zij daarop een beroep doen?	
5.	**Informeer** Hoe organiseer je dat betrokkenen weten welke persoonsgegevens waarom verwerkt worden en wat hun rechten zijn?	
6.	**Verwijder** Hoe zorg je ervoor dat gegevens zo kort mogelijk bewaard blijven en zo veel mogelijk automatisch verwijderd worden na afloop van de bewaartermijn? Denk ook aan back-ups!	
7.	**Verwerk veilig** Hoe zorg je voor scheiding en/of bundeling (aggregatie) van gegevens, zodat ze niet of moeilijker herleidbaar zijn? Anonimiseer/pseudonimiseer als dat kan!	
8.	**Vertrouwen creëren en monitoren** • Hoe geef je de eigenaar van de persoonsgegevens waar mogelijk de regie over de eigen gegevens? • Hoe leg je het privacybeleid mbt het (nieuwe) ontwerp vast en dwing je dit af? • Hoe kan je aantonen dat privacy vriendelijk met persoonsgegevens wordt omgegaan, bijvoorbeeld door monitoring, logging of audits?	
9.	**Check en leg vast** • Check of het hele ontwerp onder de loep genomen is en de bescherming van persoonsgegevens straks voldoende geborgd en aantoonbaar is. • Leg alles vast in het verwerkingsregister, procesbeschrijvingen etc.	

* is ook als Word document beschikbaar