Ministerie van Volksgezondheid,
Welzijn en Sport

THEMADOSSIER AVG

MINISTERIE VAN VWS

Colofon

Auteur	:	Directie Informatiebeleid - CIO
Bezoekadres	:	Parnassusplein 5, 2511VX, Den Haag
Contact	:	Programmateam AVG@VWS
E-mailadres	:	dienstpostbusavg@minvws.nl
Versie	:	maart 2018

Inhoud

Leeswijzer 4

1. Verwerkingsverantwoordelijke/verwerker (artikel 4 AVG) 6

1.1 Verwerkingsverantwoordelijke 6

1.2 Verwerker 6

2. Risicovolle verwerking 8

2.1 Criteria risicovolle verwerking 8

2.1.1 Evaluatie of scoretoekenning, met inbegrip van profielbepaling en voorspelling: 8

2.1.2 Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg 9

2.1.3 Stelselmatige monitoring 9

2.1.4. Gevoelige gegevens of gegevens van zeer persoonlijke aard 9

2.1.5. Op grote schaal verwerkte gegevens 9

2.1.6. Matching of samenvoeging van datasets 10

2.1.7. Gegevens over kwetsbare betrokkenen 10

2.1.8. Innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen 10

2.1.*9.* Wanneer als gevolg van de verwerking zelf "betrokkenen [...] een recht niet kunnen uitoefenen of geen beroep kunnen doen op een dienst of een overeenkomst" (artikel 22 en overweging 91). 10

3. Verantwoordingsplicht (artikel 5, tweede lid AVG) 11

3.1 Faciliteren rechten van betrokkene 11

3.2 Voldoen aan informatieplicht 11

3.3 Inbreuk in verband met persoonsgegevens (datalekken) 12

3.4 GegevensbeschermingEffectBeoordeling (GEB/PIA) 12

3.5 Functionaris Gegevensbescherming 12

4. Grondslagen (artikel 6 AVG) 13

5. Technische en organisatorische maatregelen 14

5.1 Pseudonimisering 16

5.2 Privacy (dataprotection) by design en default 17

5.2.1 Principes van privacy (dataprotection) by design 17

5.3 Privacybeleid en privacystatement 20

5.3.1 Privacybeleid 20

5.3.2 Privacybeleid vereist 20

5.3.3 Privacystatement 20

5.3.4. Opbouw privacystatement 20

Leeswijzer

In dit document vind je meer informatie over de diverse thema's binnen de Algemene Verordening Gegevensbescherming (AVG). Tevens vind je er links naar documenten en informatie elders binnen de AVG-pagina's op Rijksoverheid.nl of op het www. Het dossier is opgesteld voor het VWS-kerndepartement, concern- en koepelorganisaties, maar bevat grotendeels informatie die ook voor andere overheidsinstellingen, burgers en bedrijven interessant is.

1. Verwerkingsverantwoordelijke/verwerker (artikel 4 AVG/ definities)

Dit thema belicht de begrippen verwerkingsverantwoordelijke en verwerker. Ook licht dit themadossier toe hoe deze begrippen in de context van het ministerie en het concern begrepen moeten worden.

2. Risicovolle verwerking (artikel 4 en artikel 35 AVG)

In dit themadossier lees je wat een verwerking is en hoe je beoordeelt of een verwerking risicovol is.

3. Verantwoordingsplicht (artikel 5, tweede lid AVG)

Naast uitleg over wat verantwoordingsplicht (accountability) inhoudt, geeft dit thema op hoofdlijnen een handreiking hoe een verwerkingsverantwoordelijke aan de verantwoordingsplicht voldoet.

4. Grondslagen toestemming, wettelijke taak (artikel 6 AVG)

De meest relevante grondslagen voor gegevensverwerking vanuit de overheid wordt in dit thema toegelicht. En ook waarom de grondslag 'toestemming' niet door de overheid gebruikt gaat worden bij de uitoefening van haar wettelijke taak.

5. Technische en organisatorische maatregelen

Onderstaande themadossiers lichten toe welke technische en organisatorische maatregelen een verwerkingsverantwoordelijke kan (laten) nemen om op een verantwoorde manier met gegevens om te gaan.

5.1 Pseudonimisering

Wat verstaan we onder pseudonimisering? Een voorbeeld en handige link naar stroomschema en expert.

5.2 Privacy (dataprotection) by design en default

Er wordt steeds vaker gebruik gemaakt van (technische) innovatie. De burger is zich er in toenemende mate bewust van keuzevrijheid en ook het zicht en controle houden op het gebruik van zijn persoonsgegevens. De AVG hanteert de principes van privacy (dataprotection) by design om deze tegenstelling te overbruggen. Dit thema licht de principes van privacy (dataprotection) by design toe.

5.3 Privacybeleid/privacystatement

Dit thema geeft antwoord op wat privacybeleid is en of je als organisatie altijd een privacybeleid moet hebben.

1. Verwerkingsverantwoordelijke/verwerker (artikel 4 AVG)

Dit themadossier belicht de begrippen verwerkingsverantwoordelijke en verwerker. Ook licht dit dossier toe hoe deze begrippen in de context van het ministerie en het concern moet worden begrepen.

De rollen verwerkingsverantwoordelijke en verwerker zijn van belang om te bepalen bij wie een betrokkene terecht kan voor het uitoefenen van zijn/haar rechten die voortvloeien uit de AVG. Na het bepalen van de rol is duidelijk wie, welke verplichtingen heeft vanuit de AVG. Na een korte beschrijving volgt een vergelijking met de rollen die binnen de overheid/informatievoorziening gangbaar zijn. Besloten wordt met het duiden van de rollen verwerkingsverantwoordelijke en verwerker in het licht van het ministerie en het concern.

1.1 Verwerkingsverantwoordelijke

Een verwerkingsverantwoordelijke bepaalt doel en middelen van het verwerken van persoonsgegevens en legt hierover verantwoording af (zie ook artikel 4 AVG). De verwerkingsverantwoordelijke moet ook voldoen aan de plichten van de AVG. Dan hebben we het over de verantwoordingsplicht, het faciliteren van het uitoefenen van de rechten van betrokkenen en het invullen van de technische en organisatorische maatregelen.

1.2 Verwerker

Een verwerker verwerkt persoonsgegevens voor een verwerkingsverantwoordelijke (zie ook artikel 4 AVG). Meestal geeft de verwerker in praktische zin uitvoering aan de rechten van betrokkene. De verwerker voert de technische en organisatorische maatregelen door. Hierdoor vindt het verwerken van persoonsgegevens op een zorgvuldige en verantwoorde manier plaats.

De verwerker moet ervoor zorgen dat de verwerkingsverantwoordelijke aan zijn/haar verplichtingen van de AVG kan voldoen. In afspraken tussen verwerkingsverantwoordelijke en verwerker kan bijvoorbeeld opgenomen zijn dat een betrokkene zich tot een verwerker kan richten voor een verzoek om rectificatie of inzage.

Als verwerker moet je garanderen dat je aan de AVG voldoet bij het verwerken van persoonsgegevens. Ook moet je garanderen dat de bescherming van de rechten van betrokkene gewaarborgd zijn.

Gangbare rollen binnen de overheid zijn:

1. Opdrachtgever: zoals daar zijn ministerie en zelfstandig bestuursorgaan (ZBO);
2. Opdrachtnemer: veelal een zelfstandig bestuursorgaan of een agentschap. Het kan ook een commerciële partij zijn;
3. Leverancier: Shared Service achtige organisaties binnen de overheid en commerciële partijen.

De opdrachtgever heeft meestal de rol van verwerkingsverantwoordelijke, omdat deze het doel en de middelen van de verwerking van persoonsgegevens bepaalt.
Een opdrachtnemer en leverancier hebben in de regel de rol van verwerker, omdat deze namens de opdrachtgever daadwerkelijk de persoonsgegevens verwerkt.

Voor het ministerie van VWS en haar uitvoeringsorganisaties is het volgende van belang:

- Binnen VWS is de minister van VWS de verwerkingsverantwoordelijke;
- Zelfstandige bestuursorganen (ZBO's), zoals het Centraal Administratie Kantoor (CAK) en de Nederlandse Zorgautoriteit (NZa), kunnen verwerker voor de minister zijn. Zij hebben een eigenstandige juridische entiteit. Dit geldt ook voor commissies en raden;
- Agentschappen, zoals het RIVM en het CIBG vallen volledig onder het ministerie van VWS en kunnen daarom geen verwerker zijn voor werkzaamheden die ze voor het ministerie van VWS uitvoeren. Het feit dat de daadwerkelijke verwerking van persoonsgegevens bij agentschappen plaatsvindt in opdracht van het ministerie maakt dan niet uit. In die situaties is het van belang dat agentschappen en het ministerie/beleidsdirecties afspraken maken op welke manier voldaan kan worden aan de verplichtingen uit de AVG. Maar ook wanneer van welk organisatieonderdeel wat verwacht wordt.

Zie ook: Autoriteit Persoonsgegevens & verantwoordingsplicht

2. Risicovolle verwerking

In dit themadossier lees je wat een verwerking is en hoe je beoordeelt of een verwerking risicovol is.

Zonder er erg in te hebben verwerkt een organisatie al snel persoonsgegevens. Want verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen en raadplegen valt allemaal onder het begrip verwerking. Soms niet zonder risico. Bij verwerking van persoonsgegevens kunnen bijvoorbeeld fouten gemaakt worden. Gegevens kunnen kwijtraken of gestolen worden.

Het is van belang te weten of je verwerking risicovol (De AVG en de werkgroep artikel 29 houden het begrip hoog risico aan) met zich meebrengt. Het bepaalt mede of het uitvoeren van een verwerking een **G**egevensbescherming**E**ffect**B**eoordeling (GEB – was voorheen een PIA) moet worden.

Zie ook: model gegevensbeschermingseffectbeoordeling rijksdienst (PIA)

2.1 Criteria risicovolle verwerking

Een verwerking is risicovol als twee of meer van de volgende criteria van toepassing zijn:

2.1.1 Evaluatie of scoretoekenning, met inbegrip van profielbepaling en voorspelling:

Wanneer een organisatie kenmerken van personen gebruikt voor een evaluatie of score toekenning. Of wanneer een organisatie op basis van kenmerken van personen een profiel bepaalt om te voorspellen hoe groot een bepaald risico kan zijn. Het gaat dan met name om de volgende kenmerken:

- Beroepsprestaties;
- Economische situatie;
- Gezondheid;
- Persoonlijke voorkeuren of interesses;
- Betrouwbaarheid of gedrag;
- Locatie of verplaatsingen van de betrokkene (overwegingen 71 en 91).

Voorbeelden van een evaluatie of scoretoekenning zijn:

- Een financiële instelling die haar klanten screent op basis van een kredietreferentiedatabank;
- Een databank die wordt ingezet in de strijd tegen witwaspraktijken en terrorismefinanciering;
- Een fraudedatabank;
- Een biotechnologiebedrijf dat rechtstreeks aan consumenten genetische tests aanbiedt om ziekte-/gezondheidsrisico's te beoordelen en te voorspellen;
- Een bedrijf dat gedrags- of marketingprofielen opstelt op basis van het gebruik van of de navigatie op zijn website.

2.1.2 Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg.

De verwerking kan bijvoorbeeld leiden tot uitsluiting of discriminatie van natuurlijke personen. Verwerking met weinig of geen gevolg voor natuurlijke personen voldoet niet aan dit specifieke criterium. Verdere uitleg over deze begrippen wordt verstrekt in de komende WP29-richtsnoeren inzake geautomatiseerde individuele besluitvorming en profielbepaling.

2.1.3 Stelselmatige monitoring

Stelselmatige monitoring is het observeren, monitoren of controleren van betrokkenen, inclusief via netwerken verzamelde gegevens of "stelselmatige [...] monitoring van openbaar toegankelijke ruimten" (artikel 35, lid 3, onder c). Een voorbeeld hiervan is: cameratoezicht in een ziekenhuis of sportstadion.

Dit type monitoring is een criterium omdat de persoonsgegevens kunnen worden verzameld in omstandigheden waarin de betrokkenen mogelijk niet weten wie hun gegevens verzamelt en hoe die gegevens zullen worden gebruikt. Bovendien kan het voor natuurlijke personen onmogelijk zijn om te voorkomen dat ze aan een dergelijke verwerking in een openbare (of openbaar toegankelijke) ruimte worden onderworpen.

2.1.4. Gevoelige gegevens of gegevens van zeer persoonlijke aard

Het gaat hier om bijzondere persoonsgegevens en strafrechtelijke gegevens, zoals bedoeld in artikel 9 en 10 van de AVG. Een voorbeeld hiervan is een algemeen ziekenhuis dat medische dossiers van patiënten bewaart of een privédetective die gegevens van overtreders bewaart.

Daarnaast kan de verwerking van andere gegevenscategorieën als risicovolle verwerking worden beschouwd. Deze persoonsgegevens worden als gevoelig (zoals deze term algemeen wordt begrepen) beschouwd omdat:

- ze verband houden met huishoudelijke en privéactiviteiten (zoals elektronische communicatie, waarvan de vertrouwelijkheid moet worden beschermd);
- ze de uitoefening van een grondrecht beïnvloeden (zoals locatiegegevens waarvan de verzameling de vraag opwerpt in hoeverre de vrijheid van verkeer belemmerd wordt);
- de schending ervan duidelijk gevolgen heeft voor het dagelijkse leven van de betrokkene (zoals financiële gegevens die kunnen worden gebruikt voor betalingsfraude).

In dit opzicht kan het relevant zijn of de gegevens al openbaar zijn gemaakt door de betrokkene of door derden. Het feit dat persoonsgegevens openbaar zijn, kan als een factor worden beschouwd bij de beoordeling of de gegevens naar verwachting verder worden gebruikt voor bepaalde doeleinden. Dit criterium kan ook betrekking hebben op gegevens zoals persoonlijke documenten, e-mails, dagboeken, notities uit e-readers met notitiefuncties, en zeer persoonlijke informatie in 'life-logging-applicaties'.

2.1.5. Op grote schaal verwerkte gegevens

Bij het beoordelen of er sprake is van grootschalige verwerking van persoonsgegevens, zijn de volgende factoren van belang:

a. het aantal betrokkenen: hetzij als een specifiek aantal, hetzij als een deel van de relevante populatie;

b. het volume van gegevens en/of het bereik van verschillende gegevensitems die worden verwerkt;
c. de duur of het permanente karakter van de gegevensverwerkingactiviteit;
d. de geografische omvang van de verwerkingsactiviteit.

2.1.6. Matching of samenvoeging van datasets

Bijvoorbeeld datasets die voortkomen uit twee of meer gegevensverwerkingen die voor verschillende doeleinden zijn uitgevoerd en/of door verschillende verwerkingsverantwoordelijken zijn uitgevoerd. Waarbij een betrokkene redelijkerwijs niet hoeft te verwachten dat deze datasets samengevoegd worden.

Voorbeeld:

Als restauranthouder word je geconfronteerd met een extra controle van de NVWA, omdat zij de recensies van de website Iens hebben gekocht.

2.1.7. Gegevens over kwetsbare betrokkenen

De verwerking van dit soort gegevens is een criterium vanwege de toegenomen machtsongelijkheid tussen de betrokkenen en de verwerkingsverantwoordelijke. Dat kan betekenen dat natuurlijke personen niet in staat zijn gemakkelijk in te stemmen met of bezwaar te maken tegen de verwerking van hun gegevens, of om hun rechten uit te oefenen. Voorbeeld kwetsbare betrokkenen zijn:

- kinderen: zij zijn niet in staat bewust en bedachtzaam in te stemmen met of bezwaar te maken tegen de verwerking van hun gegevens;
- werknemers;
- kwetsbaardere segmenten van de bevolking die speciale bescherming behoeven, zoals geesteszieken, asielzoekers, bejaarden, patiënten enz. In elk geval waarin een onevenwichtigheid in de relatie tussen de positie van de betrokkene en de verwerkingsverantwoordelijke kan worden vastgesteld.

2.1.8. Innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen

Hierbij hebben we het over de combinatie van het gebruik van vingerafdrukken en gezichtsherkenning voor een betere fysieke toegangscontrole.

Ook wanneer voor het verwerken van persoonsgegevens gebruikt wordt gemaakt van nieuwe technologie, kan deze verwerking een hoog risico met zich meebrengen. Dit komt omdat het gebruik van dergelijke technologie nieuwe vormen van gegevensverzameling en -gebruik kan inhouden. Mogelijk met een hoog risico voor de rechten en vrijheden van natuurlijke personen. De persoonlijke en sociale gevolgen van het gebruik van een nieuwe technologie kunnen immers onbekend zijn.

2.1.9. Wanneer als gevolg van de verwerking zelf "betrokkenen [...] een recht niet kunnen uitoefenen of geen beroep kunnen doen op een dienst of een overeenkomst" (artikel 22 en overweging 91).

Hierbij hebben we het over verwerkingen die erop gericht zijn de toegang van betrokkenen tot een dienst te wijzigen of te wijzigen. Dat geldt ook bij de mogelijkheid van betrokkenen om een overeenkomst aan te gaan toe te staan. Een voorbeeld hiervan is een bank die zijn klanten screent op basis van een databank met kredietreferenties om te beslissen of ze al dan niet een lening aangeboden krijgen.

3. Verantwoordingsplicht (artikel 5, tweede lid AVG)

Naast uitleg over wat verantwoordingsplicht (accountability) inhoudt, geeft dit thema op hoofdlijnen een handreiking hoe een verwerkingsverantwoordelijke aan de verantwoordingsplicht voldoet.

Volgens het Europese Comité voor gegevensbescherming integreert de AVG de 'verantwoordingsplicht' als een principe dat vereist dat organisaties passende technische en organisatorische maatregelen nemen om persoonsgegevens te beschermen. Daarbij moeten organisaties ook in staat zijn dit te laten zien en aan te tonen in welke mate de genomen maatregelen effectief zijn. Kortom, organisaties moeten kunnen aantonen dat zij aan de verplichtingen van de AVG voldoen.

De verantwoordingsplicht is expliciet opgenomen in artikel 5, tweede lid AVG. Daarnaast vereist de AVG onder voorwaarden het uitvoeren van een gegevensbeschermingeffectbeoordeling (artikel 35 AVG) en het aanstellen van een Functionaris Gegevensbescherming (artikel 37 AVG).

3.1 Faciliteren rechten van betrokkene

Dit kan met behulp van een privacy statement/beleid in algemene zin en, wanneer nodig, op maat naar de betrokkene toe. In een privacy statement/beleid staat minimaal het soort verwerkingen dat een organisatie verwerkt en de grondslagen op basis waarvan die mogen worden verwerkt. Maar ook de doelen waarvoor de gegevens worden verwerkt, de rechten van betrokkenen en op welke wijze zij die effectief kunnen gebruiken. Het privacy statement van de Autoriteit Persoonsgegevens is bijvoorbeeld kort, bondig en duidelijk.

3.2 Voldoen aan informatieplicht

Ook hier kan een privacy statement/beleid in algemene zin helpen. Tevens kan een verwerkingsverantwoordelijke in een concrete situatie een betrokkene informatie geven over de soort verwerkingen en de grondslagen op basis waarvan die mogen worden verwerkt. Maar ook de doelen waarvoor de gegevens worden verwerkt, de rechten van betrokkenen en op welke wijze zij die kunnen gebruiken.

Passende technische en organisatorische maatregelen
Het zorgvuldig en op een verantwoorde manier verwerken van persoonsgegevens. De verwerkingsverantwoordelijke toont dat aan door in algemene zin te communiceren welke technische en organisatorische maatregelen genomen zijn ter bescherming van de informatieveiligheid Een voorbeeld hiervan zijn NEN-normen. Daarnaast helpen periodieke interne en externe audits. Als een verwerkingsverantwoordelijke kan laten zien dat het in actie komt na een veiligheidsincident en daarbij tevens laat zien dat de actie effect heeft gehad, toont een verwerkingsverantwoordelijke aan dat hij voldoet aan de verplichtingen die de AVG oplegt.

Zie voor een inhoudelijke toelichting het themadossier: Technische en organisatorische maatregelen.

3.3 Inbreuk in verband met persoonsgegevens (datalekken)

Wanneer een verwerkingsverantwoordelijke in haar privacybeleid/statement in algemene zin aangeeft op welke manier hij omgaat met datalekken, helpt dat bij het voldoen aan de verantwoordingsplicht.

3.4 GegevensbeschermingEffectBeoordeling (GEB/PIA)

De verwerkingsverantwoordelijke voldoet aan de verantwoordingsplicht door periodiek risico's in kaart brengen over het verwerken van persoonsgegevens. En naar aanleiding van deze inventarisatie onderneemt deze persoon ook acties. Zeker als een verwerkingsverantwoordelijke in algemene zin aangeeft wanneer deze PIA's laat uitvoeren.

3.5 Functionaris Gegevensbescherming

In je privacybeleid opnemen hoe de 'privacy' qua taken, rollen en bevoegdheden ingericht is, helpt bij het voldoen aan de verantwoordingsplicht. De Functionaris Gegevensbescherming is één van de rollen die in dit kader relevant is.

4. Grondslagen (artikel 6 AVG)

De meest relevante grondslagen voor gegevensverwerking vanuit de overheid worden in dit thema toegelicht. Maar ook waarom de grondslag 'toestemming' niet door de overheid wordt gebruikt bij de uitoefening van haar wettelijke taak.

De AVG noemt in artikel 6 de redenen waarom persoonsgegevens verwerkt mogen worden. Bij het uitoefenen van hun publieke taken maken overheden in de regel gebruik van de grondslagen:

- uitoefenen wettelijke verplichting;
- een taak van algemeen belang;
- een taak in het kader van de uitoefening van het openbaar gezag.

Overheden mogen bij het uitoefenen van hun wettelijk en publieke taken geen gebruik maken van de grondslag: 'gerechtvaardigde belangen'. Reden hiervoor is dat het aan de wetgever is om de rechtsgrond voor verwerking van persoonsgegevens door overheden te creëren.

Ook van de 'grondslag toestemming' maken overheden bij het uitoefenen van hun wettelijke/publieke taken weinig tot geen gebruik. Reden hiervoor is dat in de relatie overheid-burger, de burger vaak geen alternatief heeft. Dan is er geen sprake van 'vrij gegeven' toestemming.

De 'grondslag toestemming' speelt in het zorgveld wel een belangrijke rol.

- Meer informatie vind je op Rijksoverheid.nl

5. Technische en organisatorische maatregelen

De AVG spreekt over technische en organisatorische maatregelen om de fundamentele rechten en vrijheden van burgers over gegevensbescherming te faciliteren. Dit themadossier behandelt een aantal van de maatregelen die een organisatie kan nemen.

Organisaties moeten passende technische en organisatorische maatregelen treffen om de persoonsgegevens die zij verwerken te beveiligen.

> ***Technische maatregelen*** *zijn alle maatregelen die zonder menselijk ingrijpen een beveiligings- of toegangsaspect afdwingen (voorbeeld toegang via gebruikernaam en wachtwoord of encryptie).*
>
> ***Organisatorische maatregelen*** *zijn maatregelen met menselijk toezicht, zoals een portier die bezoekers identificeert.*
>
> *(bron: boek > De Algemene Verordening Gegevensbescherming – Artikelsgewijs commentaar – Arnoud Engelfriet, Lisette Chew-Meij en Peter Kager. Editie 2017)*

Om tot 'passende technische en organisatorische maatregelen' te komen beoordeelt een organisatie of en zo ja welke risico's verbonden zijn aan het verwerken van persoonsgegevens.

Factoren die een rol kunnen spelen in deze beoordeling zijn:

- de schade die kan optreden als gevolg van het verwerken van persoonsgegevens;
- de ernst van de schade;
- de waarschijnlijkheid dat de schade ontstaat.

Voorbeelden van verwerkingen waarbij schade kan ontstaan:

- als de verwerking leidt tot discriminatie;
- als de verwerking tot gevolg heeft dat betrokkene hun rechten niet kunnen uitoefenen;
- als bijzondere persoonsgegevens worden verwerkt;
- als persoonsgegevens van kwetsbare natuurlijke personen, zoals bijvoorbeeld kinderen, worden verwerkt.

Bij het beoordelen van de ernst van de schade en de waarschijnlijkheid dat de schade ontstaat, zijn de volgende factoren van belang:

- de aard van de persoonsgegevens (persoonsgegevens of bijzondere persoonsgegevens);
- het toepassinggebied van de verwerking;
- de context waarin de verwerking plaatsvindt;
- de doeleinden van de verwerking.

Op basis van deze beoordeling bepaalt een organisatie of een verwerking een risico of een hoog risico met zich meebrengt. Wanneer een verwerking een hoog risico op schade heeft, dan is een GevensbeschermingEffectBeoordeling (GEB/PIA -) verplicht.

Naar aanleiding van een belangenafweging op voorgaande aspecten, volgt een gemotiveerde keuze van maatregelen, het toepassen en uitvoeren van de maatregelen. Dit kunnen onder meer de volgende maatregelen zijn:

- de pseudonimisering en versleuteling van persoonsgegevens;
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking;
- het inrichten van een privacyorganisatie.

5.1 Pseudonimisering

Wat verstaan we onder pseudonimiseren? Een voorbeeld en handige link naar stroomschema en expert.

De AVG definieert pseudonimisering als volgt:

'Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.' (artikel 4, onderdeel 5 AVG)

Pseudonimiseren is een procedure waarmee identificerende gegevens met een bepaald algoritme worden vervangen door versleutelde gegevens (het pseudoniem).

Bijvoorbeeld
Piet Jansen krijgt de code: 1@3fg56HH. Dit gebeurt met bijvoorbeeld encryptie. Na de encryptie is de verantwoordelijke nog steeds in staat om de betrokkene te identificeren. De gespeudonimiseerde persoonsgegevens zijn nog steeds persoonsgegevens. Pseudonimisering zorgt er voor dat bij een datalek misbruik van de gegevens kleiner wordt.

Zie ook document: stroomschema pseudonimisering

Een organisatie die expert is in het pseudonimiseren is ZorgTTP.

5.2 Privacy (dataprotection) by design en default

Er wordt steeds vaker gebruik gemaakt van (technische) innovatie. De burger is zich er in toenemende mate bewust van keuzevrijheid en ook het zicht en controle houden op het gebruik van zijn persoonsgegevens. De AVG hanteert de principes van privacy (dataprotection) by design om deze tegenstelling te overbruggen. Dit thema licht de principes van privacy (dataprotection) by design toe.

Privacy by design is een verzameling principes waarmee je op een zorgvuldige en verantwoorde manier privacy meeneemt in de ontwikkeling en het gebruik van het verwerken van persoonsgegevens.

5.2.1 Principes van privacy (dataprotection) by design

Naast de specifieke principes van privacy by design zijn ook algemene principes als evenredigheid en proportionaliteit van belang bij een beoordeling welke maatregelen je als organisatie neemt of juist niet neemt.

1. **Proactief en preventief in plaats van reactief en herstellend**
   Privacy by Design geldt vanaf de start van het ontwerp van een systeem en niet achteraf. Ontwerp is in dit kader een ruim begrip. Vanuit overheid betekent ontwerp: vanaf het moment van wetgeving en beleidsvorming.

2. **Privacy by default**
   Systemen / voorzieningen zijn zo ingericht dat deze standaard op privacyvriendelijk staan. Privacy by default streeft dan naar een maximale privacy door te verzekeren dat persoonsgegevens in een IT-systeem automatisch afdoende beschermd zijn. Bij privacy by default geldt ook het principe: pas toe of leg uit (comply or explain).

3. **Privacy geïntegreerd in het ontwerp**
   Privacymaatregelen zijn integraal onderdeel van de informatieverwerking en zijn geen extra functionaliteiten in het systeem (add-on). Dit geldt voor de technische systemen én de organisatorische processen. Dit is vergelijkbaar met principe 1.

4. **Volledige functionaliteit – win/win in plaats van compromissen**
   Als je 'privacy' meeneemt vanaf het ontwerp leidt dat tot 'volledige' functionaliteit. Er is dan weloverwogen een keus gemaakt in 'volledigheid'. Vergelijk het met de keuze voor een Lada of een Mercedes. Op het moment dat je weloverwogen gekozen hebt voor een Lada, dan is dat je volledige functionaliteit. Als je dan functionaliteit van Mercedes zou inbouwen in een Lada krijg je naar alle waarschijnlijkheid een slechtere Lada.

   Privacy by Design streeft ernaar om alle legitieme belangen en doelstellingen op de wijze van een 'win-win' te faciliteren, en niet op ouderwetse wijze met elkaar te verzoenen door middel van compromissen waar die niet nodig zijn.

5. **Bescherming tijdens de volledige levenscyclus**
   Privacy by Design, geïntegreerd in een systeem nog voordat er enige informatie is verzameld, strekt zich uit over de gehele levenscyclus van de betrokken gegevens.

Welke maatregelen neem je tijdens ontwerp, gebruik, uitfaseren. Heb hierbij, indien van toepassing, ook aandacht voor persoonsgegevens in de Cloud.

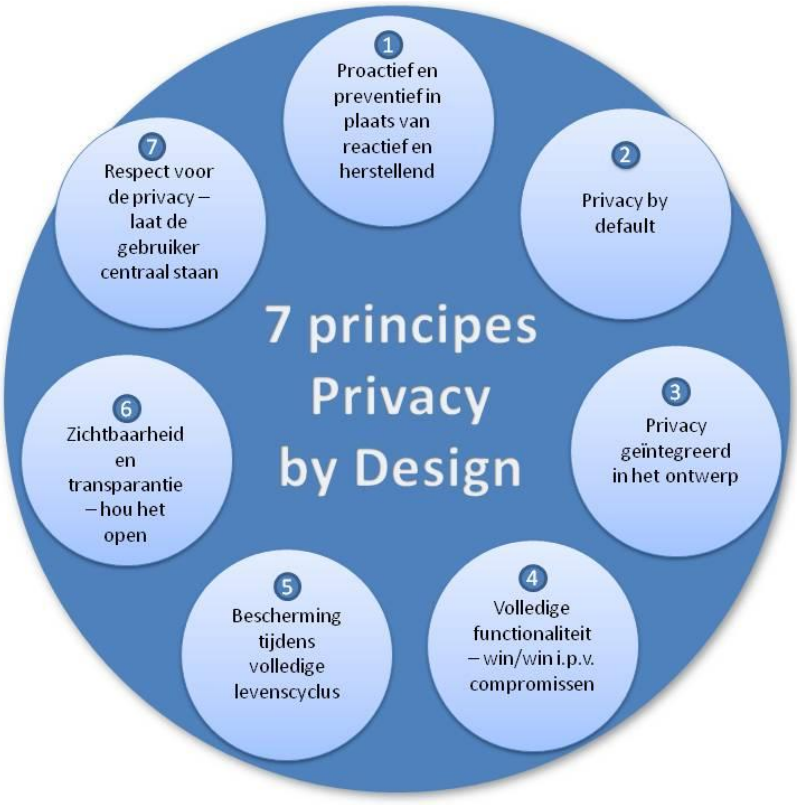
6. **Zichtbaarheid en transparantie – hou het open**
   Inzicht en transparantie over hoe persoonsgegevens worden verwerkt is binnen de wet- en regelgeving een criterium en moet mogelijk gemaakt worden voor de betrokkene, eenieder, de eigen organisatie en toezichthouders.
   Zorg voor effectieve procedures voor burgers zodat zij inzicht en controle over hun persoonsgegevens kunnen uitoefenen.

7. **Respect voor de privacy – laat de gebruiker centraal staan**
   Privacy by design heeft zijn doel pas bereikt, wanneer het (binnen de context van de verwerking van persoonsgegevens) daadwerkelijk zorg draagt voor de bescherming van de persoonlijke levenssfeer. Niet het toepassen of uitvoeren van een maatregel is hierbij leidend, maar het beoogde resultaat voor de betrokkene. Bij iedere maatregel moet daarom verder gekeken worden dan alleen het uitvoeren ervan: er moet vastgesteld worden of het beoogde resultaat voor de betrokkene zich daadwerkelijk voordoet.

   De uitdaging: salans vinden tussen met zo min mogelijk maatregelen het meeste effect weten te bereiken. Let hierbij er ook op wie de maatregelen bepaalt en wie de maatregelen betaalt.

Zie ook: Handleiding Privacy by Design - versie 3.0

De genoemde 7 principes zien er in een **infografi**c zo uit:




Privacy by Design tools
Mobiele apparaten
• Toegang tot persoonsgegevens
• bescherming van persoonsgegevens
• Privacy bescherming
Privacy enhancement technologieën
• Ondersteuning organisatorische processen
• Ondersteuning technische gegevensverwerking
Passende granualiteit
• Gegevenslaag
• Verwerkingslaag
• Proces besturingslaag
Gegevens-management
• Meta gegevens
•Tags
•File analyse
Kwaliteits-management
• Voorkom onjuiste gegevens
• Controle en correctie door betrokkene
Identity en Access Management
•Authenticatieservice
•Autorisatiemana-gement
•Toestemmingsmana-gement
Bewaren van persoonsgegevens
• Single point of truth
• Bewaartermijn
• Vernietigen
Veilige doorgifte
• Data loss prevention
• Cloud data protection gatewa
• E-mail encryptie
Doorgifte persoonsgegevens
• Onderling vertrouwen
• Koppelingen
• Locatie
• Pseudonimisering
• Openheid
Veilige opslag
• Database-encryptie
•Limited Disclosure
•Technology Logging and monitoring
•Tokenization
•Datamasking
•Triple blind encryptie
•Gegevens wiping

5.3 Privacybeleid en privacystatement

Dit thema beschrijft wat privacybeleid en of het een vereiste is. Daarnaast leggen we het begrip privacystatement kort uit.

5.3.1 Privacybeleid

Een verwerkingsverantwoordelijke kan ervoor kiezen om alle technische en organisatorische maatregelen die hij neemt om te waarborgen en aan te tonen dat hij aan de AVG voldoet, uitwerken in een beleid: het privacybeleid.

5.3.2 Privacybeleid vereist

Het maken van privacybeleid is alleen vereist wanneer dat in verhouding staat tot de betreffende verwerkingen. Bij een eenvoudige verwerking is het opstellen van uitgebreide beleidsdocumenten niet verplicht. Het is aan de verwerkingsverantwoordelijke om te bewijzen dat hij aan de AVG voldoet. Het hebben van een geïmplementeerd privacybeleid is één van de wegen die bewandeld kan worden.

In het privacybeleid documenteert een organisatie hoe deze omgaat met privacy, zowel organisatorisch als technisch. Het maken van algemeen beleid dat de naleving van de AVG op hoofdlijnen beschrijft heeft de voorkeur. In dit gedeelte beschrijft een organisatie de doelen waarvoor de persoonsgegevens worden verwerkt en de stappen ter beveiliging daarvan tot de wijze waarop betrokkene hun rechten kunnen uitoefenen. Hierna kan een organisatie specifieke aanvullingen opnemen voor de verschillende gebieden.

Het privacybeleid is een intern document van en voor de betreffende organisatie.

5.3.3 Privacystatement

Een privacystatement is een document bedoeld voor de betrokkenen waarin staat:

1. welke organisatie persoonsgegevens van betrokkene verwerkt;
2. welke persoonsgegevens worden verwerkt;
3. met welk doel de persoonsgegevens van betrokkene worden verwerkt;
4. wie de Functionaris Gegevensbescherming is van de organisatie die de persoonsgegevens van de betrokkene verwerkt;
5. hoe lang gegevens bewaard worden;
6. welke rechten betrokkene hebben ten aanzien van de verwerking van hun persoonsgegevens;
7. de grondslag van de verwerking (bijvoorbeeld: wet, toestemming, uitvoering van een overeenkomst);
8. of de persoonsgegevens gebruikt worden voor automatische besluitvorming, met inbegrip van profilering.

5.3.4. Opbouw privacystatement

De informatie over de gegevensverwerking moet beknopt, transparant en begrijpelijk zijn. Duidelijke en eenvoudige taal is een eis. Om de informatie in een (online) privacyverklaring zo toegankelijk mogelijk te maken, kan de verklaring in meerdere lagen opgesteld worden.

Bijvoorbeeld

- In de eerste laag geeft u kort aan wie de verantwoordelijke organisatie is, hoe die te bereiken is en welke gegevensverwerkingen de meeste impact hebben op de betrokken personen.

- In de tweede en derde laag van de privacyverklaring kunt u meer in detail aangeven welke persoonsgegevens u voor welk doel verwerkt en hoe mensen hun rechten kunnen uitoefenen.