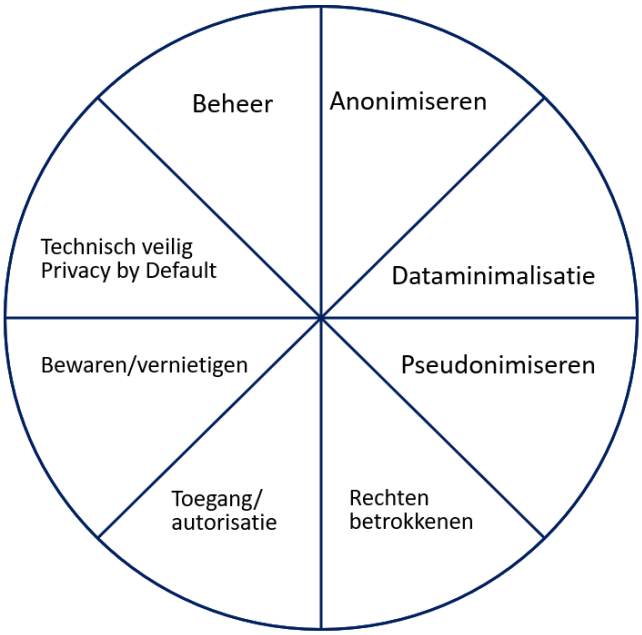
Samen aanjagen van vernieuwing

Privacy by Design

Handreiking voor het onderwijs



Colofon

Voor personen zonder specialistische kennis is het begrip ‘Privacy by Design’ vaak nogal abstract. Dit document geeft handvatten om het begrip Privacy by Design (zoals vereist volgens artikel 25 van de Algemene Verordening Gegevensbescherming) te verduidelijken.

Het document past bij Toetsingskader Privacy, statement PR.06 (Privacy by Design).

Bestemd voor

Dit document is bestemd voor mensen die met persoonsgegevens werken in de onderwijssector, specifiek voor privacy- en securityprofessionals.

Samenstelling en beheer

Dit document is tot stand is gekomen via het Privacy Expertise Centrum van SURF. Het is gebaseerd op van de literatuur van privacy-expert Ann Couvakian, Privacyontwerpstrategieën (Het Blauwe Boekje) van Jaap-Henk Hoepman en het Framework Privacy by Design dat is samengesteld door het Nederlandse bedrijf Privacy Company. Het beheer van deze handreiking berust bij SURF.

Licentie

Dit document is verstrekt onder de creative commons-licentie CC BY-NC-SA 4.0 © 2021 by Helma de Boer (werkgroep mbo). SURF aanvaardt geen aansprakelijkheid voor enig gebruik/toepassing van dit document.

Versiebeheer

Versie	Door	Datum	Toelichting/wijziging
1.0	Privacy Expertise Centrum, Helma de Boer	25-08-2025	n.v.t.

Inhoudsopgave

1 Inleiding

Privacy by Design is de ruggengraat van de gegevensbescherming zoals bedoeld in de Algemene Verordening Gegevensbescherming (AVG). In de praktijk blijkt echter dat het begrip als abstract wordt ervaren. Als niet duidelijk is wat er moet worden gedaan om het concept toe te passen, is het risico groot dat er niets mee wordt gedaan. Dit document helpt het concept Privacy by Design beter te doorgronden en drempels voor toepassing ervan te verlagen.

2 Uitgangspunten

Definitie Privacy by Design

Privacy by Design is een principe waarin privacybescherming vanaf het begin wordt meegenomen bij het ontwerpen en bouwen van nieuwe systemen en/of processen. Het bestaat uit het formuleren van privacycriteria in het ontwerp van een systeem of proces en afstemming daarover met ontwerpers en beheerders, om redelijkerwijs bescherming te bieden tegen storingen en ongeoorloofde toegang. Op die manier kan privacy in een vroeg stadium worden verankerd.

Dat gaat níet alleen over technische beschermingsmaatregelen/techniek, maar ook over organisatorische. In dit document worden deze twee soorten beschermingsmaatregelen per onderwerp door elkaar behandeld (zie bijlage 3 voor het onderscheid).

Het framework Privacy by Design[1] is een manier van werken die volgt uit zeven fundamentele, internationaal erkende privacyprincipes van Ann Couvakian:

1. Proactief en preventief werken aan privacybescherming (niet reactief/oplossend)
2. Privacy is standaard
3. Privacy is in het ontwerp verwerkt
4. Volledige functionaliteit wordt geboden (met security èn privacy)
5. Volledige bescherming van begin tot eind
6. Zichtbaar en transparant
7. De gebruiker staat centraal

Het is belangrijk dat een medewerker als gebruiker zonder hindernissen het werk moeten kunnen doen (de gebruiker staat centraal en kan alle functionaliteit gebruiken die nodig is om het werk uit te voeren).

De AVG gaat ervan uit dat Privacy by Design steeds voldoet aan de ‘stand der techniek’. Je moet mee met de tijd. Dat betekent dat er continu moet worden bekeken of een bepaalde bescherming ondertussen kan worden verbeterd en – als dat proportioneel is, want het kostenplaatje speelt ook mee - moet worden verbeterd.

[1] Framework volgens Privacy Company

Het verschil met Privacy by Default

Privacy by Default gaat over de instellingen in een systeem zelf. De configuratie moet standaard zo zijn ingesteld dat er standaard sprake is van privacybescherming. De eindgebruiker hoeft daarvoor zelf niets meer extra in te stellen. De complexiteit van een privacyconfiguratie moet dus geen probleem voor de gebruiker zijn. Denk bijvoorbeeld aan een goede gebruikersinterface, duidelijke en opt-in voor het delen van gegevens in plaats van op-out.

3 Zo werkt het concreet

Het framework Privacy by Design (zie ook bijlage 2) volgt acht stappen in een vaste volgorde:

1. Werk met anonieme gegevens als dat kan
2. Verzamel zo weinig mogelijk
3. Pseudonimiseer waar dat kan
4. Zorg voor versleuteling
5. Regel het toegangsbeheer goed
6. Gegevensbescherming is standaard
7. Borg de bewaar- en vernietigingstermijnen
8. Faciliteer de rechten van betrokkenen

Daarna: zorg voor management (beheer)

Stap 1 – Werk met anonieme gegevens

De AVG is alleen van toepassing op persoonsgegevens.[2] Privacy by Design kent daarom als eerste stap: het verwerken van anonieme gegevens. Als gegevens op geen enkele manier terug kunnen leiden naar een individu, is er geen sprake van persoonsgegevens. Als het niet nodig is om te weten van wie gegevens afkomstig zijn, verwerk je de gegevens anoniem. De AVG is daar niet op van toepassing.

Tactieken

- Anoniem verzamelen – werk niet met accounts, maar b.v. met een sleutel (unieke code die niet te herleiden is aan een specifieke persoon), en een openbare url. Een goed voorbeeld van anoniem verzamelen is privacy-friendly.nl/dpia
- Anoniem verwerken – als je de identiteit kent: koppel de identifiers los van de antwoorden (en sla ze bij voorkeur niet op, maar gooi ze weg na het loskoppelen, bijvoorbeeld bij enquêtes). Als persoonsgegevens zo zijn gepseudonimiseerd dat het onevenredig veel inspanning kost om de koppeling weer tot stand te brengen, kunnen de persoonsgegevens vaak ook als anoniem beschouwd. Een goed voorbeeld van anoniem verwerken is TestjeLeefstijl.

Anoniem verzamelen/verwerken kan alleen als er ook geen profielgegevens worden verzameld of doorgegeven via browser of app.

[2] Het is niet zonder meer toegestaan om reeds beschikbare persoonsgegevens te anonimiseren, omdat je dan gegevens 'verder verwerkt'. Dit moet voldoen aan de eisen rondom doelbinding. Daar waar het gaat over onderzoek (historisch, statistisch, wetenschappelijk) wordt overigens al snel aangenomen dat er een wettelijke verwerkingsgrondslag is.

Écht anonimiseren is een specialisme
Het goed anonimiseren van gegevens is een specialisme. Als je een bepaalde methode kiest om te anonimiseren, moet je kunnen onderbouwen dat die methode voldoende garanties biedt, zodat de data zelfs in combinatie met andere gegevens niet alsnog leidt tot identificatie van een individu.

Bijvoorbeeld: mannen van een bepaalde opleiding zijn vaker ziek dan vrouwen, maar je weet dat er slechts drie mannen zijn die die opleiding volgen; dan weet je al snel over wie het gaat. Zulke gegevens kunnen alleen in geaggregeerde vorm (grotere aantallen) anoniem blijven. Zonder heel technisch te worden: alleen wat getallen wijzigen of het inkorten van een reeks getallen is vaak niet voldoende.

Anonimiseren is in veel gevallen een taak voor een techneut.

Stap 2 – Verzamel zo weinig mogelijk

Wat je niet verzamelt, kun je ook niet kwijtraken. Verzamel niet meer dan je nodig hebt en denk er ook aan om na het verzamelen gegevens te minimaliseren als je ze niet meer nodig hebt. Bedenk steeds welke aanpak het meest privacyvriendelijk is.

Tactieken
- Selecteer wat relevant is en verzamel niet meer dan dat. Wil je een leeftijd weten, vraag dan niet naar de volledige geboortedatum.
- Sluit op voorhand uit wat je niet wilt verzamelen en gooi weg als het onverhoopt toch binnenkomt. Moet je bijvoorbeeld een ID-bewijs of diagnose controleren? Laat deze tonen en registreer de controle, maar sla geen kopie op.
- Verwijderen gegevens die niet langer nodig zijn. Dat kan bijvoorbeeld door een veld uit een record na een bepaalde periode op een standaardwaarde te zetten. Zo kan het record bruikbaar blijven voor wat je nodig hebt, terwijl gegevens die niet meer nodig zijn, zijn verwijderd.
- Vernietig wat je niet meer nodig hebt van fysieke opslagmedia (zoals USB-stick, externe harde schijf).
- Focus op de kernactiviteiten van de organisatie. Verzamel geen gegevens die niet nodig zijn of samenhangen met je diensten.
- Minimaliseer ook als je gegevens wilt delen, analyseren en verrijken. Deel bijvoorbeeld voor managementinformatie alleen de echt relevante gegevens.

Stap 3 - Pseudonimiseer waar dat kan

Pseudonimiseren maakt het mogelijk om informatie te gebruiken zonder te weten over wie het gaat, terwijl dat wel zichtbaar gemaakt kan worden. Zo kan een analist het werk doen zonder te weten om wie het gaat, maar kan iemand wel worden geïdentificeerd als dat nodig is (bijvoorbeeld vanwege uitkomsten van een medisch onderzoek). Pseudonimiseren is vaak een taak voor een techneut.

Tactieken:

- Maak gegevens abstracter door minder details te verzamelen of te tonen.
- en vat samen (toon resultaten in categorieën, zoals leeftijdscategorie in plaats van geboortedatum, woonplaats in plaats van adres)
- Aggregeer informatie over personen (gebruik een gemiddelde waarde voor profielen, toon percentages).
- Voeg ruis toe.
- Maak data onbegrijpbaar voor derden, zodat ze onleesbaar worden zonder de ontcijferingssleutel. Hash persoonsgegevens om er pseudoniemen van te maken.

Stap 4 – Zorg voor versleuteling van de gegevens

Versleuteling (encryptie) is een belangrijk technisch onderdeel van gegevensbescherming. Je gebruikt het in ieder geval als persoonsgegevens niet worden gebruikt (gegevens in opslag of onderweg). Kies bewust voor de benodigde versleutelingstechnieken voor systemen en verwerkingen.

Tactieken:

- Pas versleutelingstechnieken toe op data, zoals end-to-end, VPN, SSL, TLS, hash/salt, standaard-encryptie ‘at rest’ en/of maskeer data:

Bescherming van data	Verbergen (“masking”)	encryptie
‘in transit’ (onderweg)	Nee	Ja
‘at rest’ (in ruste)	Ja	Ja
Continu beschikbaar	Ja	Nee
Back-up	Nee	Ja

- Afhankelijk van de gevoeligheid en grootte van de verwerking mogen de decryptiesleutels niet bekend zijn bij de leverancier voor cloudopslag. Dat betekent dat er additionele versleuteling plaatsvindt voordat op het versleutelde medium wordt opgeslagen, omdat de leverancier zelf de encryptie ‘at rest’ verzorgt (en dus kan ontsleutelen). Dit is bijvoorbeeld van belang bij een grote back-up die op een server komt te staan van een Amerikaanse leverancier. Je kunt dit vergelijken met een Word-document dat je zelf versleutelt en vervolgens opslaat op de c-schijf waar Bitlocker op staat.
- Laat een pentest en/of kwetsbaarheidstest uitvoeren (check of certificaten van de server geldig zijn, controleer op onveilige functies, controleer of onveilige HTTP-verzoeken zijn toegestaan, b.v. doordat de App Transport Security is uitgeschakeld)
- Gebruik homomorfe versleuting als dat kan (b.v. rekenen met gegevens zonder de gegevens zelf te kennen). Dit wordt nog niet veel toegepast en het vergt meer rekenkracht (= kosten).

Stap 5 – Regel het toegangsbeheer goed

Toegangsbeheer bestaat uit Identity & Access Management (IAM). Het gaat concreet over identificatie, authenticatie en autorisatie. Ondanks toekenning van de juiste rollen en rechten kunnen in veel applicaties gemakkelijk persoonsgegevens uit het systeem worden gehaald voor verder gebruik.

Hierin schuilt het risico dat een medewerker persoonsgegevens exporteert en uitwisselt voor een doel dat niet is beschreven maar wel legitiem lijkt, terwijl het dat misschien niet is. Maar, misschien is het doel wel legitiem, maar is de methode niet veilig genoeg is, afhankelijk van de data in de export.

Tactieken:
- Zorg voor een goed IAM-proces (Identity and Access Management)
- Autorisatie volgens need-to-know/least privilege inrichten.
- Autorisatieschema's vaststellen.
- Afwijkende rechten volgens vierogenprincipe toekennen.
- Uitzonderingen zijn zoveel mogelijk tijdelijk.
- Gebruik technieken als Data Loss Prevention (DLP), vertrouwelijkheidslabels en Information Rights Management (IRM).
- Multifactorauthenticatie (MFA) gebruiken waar nodig.
- Rechten verwijderen als ze niet meer nodig zijn.
- De rechten CRUDIE (Create, Read, Update, Import, Export) los van elkaar toekennen. Bijvoorbeeld: iemand met alleen leesrechten 'R' kan raadplegen, maar niet downloaden. Iemand met de rechten 'RE' kan dat wel. Het ontwerp moet dit ondersteunen. Datamasking kan hier ook uitkomst bieden.
- Gegevensscheiding/partitioneren: de mogelijkheid beperken om grote hoeveelheden gegevens in een keer binnen en buiten de organisatie te verspreiden door gefragmenteerde opslag, in plaats van concentreren van alle gegevens in één database.
- Medewerkers die exporteermogelijkheden hebben, moeten aanvullend worden getraind: ze moeten weten onder welke voorwaarden en op welke manier zo'n export kan plaatsvinden.
- Zorg ervoor dat interne en externe koppelingen in beeld zijn, zodat de broneigenaar weet of een medewerker persoonsgegevens deelt met externe organisaties.
- Gebruik privacyvriendelijke credentials voor identiteitsbeheer (Attribute Based Credentials).
- Controleer of afspraken worden gevolgd.

Stap 6 – Gegevensbescherming is standaard

De verwerking van persoonsgegevens moet veilig gebeuren. Hulpmiddelen zijn:
- privacyvriendelijke instellingen als standaard (Privacy by Default), en
- informatiebeveiliging (als passend beschermingsniveau). De informatiebeveiliging moet steeds voldoen aan de stand der techniek. Dit vraagt om borging via een PDCA-proces.

De voorbeelden hieronder zijn niet uitputtend.

Tactieken:
Privacy
- Geef de gebruiker controle en maak keuzes opt-in in plaats van opt-out (cookies afwijzen, de gebruiker zelf laten kiezen welke gegevens men in een profiel wil tonen).
- Geef de gebruiker een privacydashboard met de mogelijkheid tot inzage - welke gegevens zijn er, hoe ze worden verwerkt, waarvoor en met wie dit wordt gedeeld -, correctie en verwijdering. Zie ook stap 8.
- Kies voor (leveranciers met) opslaglocaties in de EU.
- Maak afspraken over gegevensuitwisseling (VO, GUO)

- Toon een pasfoto alleen in die modules van een applicatie waar de foto noodzakelijk is voor identificatie, zoals in de aan- en afwezigheidsregistratie. In andere modules komt de foto niet beschikbaar.

Informatiebeveiliging/security
- Scheid de verwerking van persoonsgegevens (verwerk gegevens in verschillende van elkaar gescheiden databases/systemen en maak gebruik van decentrale systemen). Zo is het moeilijker om gegevens met elkaar te combineren.
- Maskeer (verberg) data en/of beperk de toegang tot gegevens (b.v. BSN maskeren als er geen leesrechten zijn).
- Gevaarlijke extensies voorkomen: bewust kiezen welke bestandstypen waar mogen worden geüpload in de systemen van de organisatie.
- Zorg voor goede logging (wie doet wat, waar en wanneer – en waarom) voor traceerbaarheid.
- Gebruik technieken die ongewone toegang en gebruik van data registreert en dat blokkeert (bijvoorbeeld voorkomen dat één persoon veel data opvraagt, of dat veel personen data van één persoon bekijken, denk aan een medisch dossier van een bekende Nederlander, of van de dochter van de directeur).
- Maak back-ups om ervoor te zorgen dat er geen persoonsgegevens verloren gaan als dat niet de bedoeling is (dit is ook een datalek).
- Pas best practices toe van informatiebeveiliging.
- Schoon gedetailleerde loginformatie op als de relevantie ervan afneemt.
- Zorg bij gevoelige verwerkingen voor een externe audit (pentest, vulnerability check).

Stap 7 – Borg de bewaar- en vernietigingstermijnen

Het is vaak niet goed duidelijk hoe in het “opruimen” wordt voorzien en hoe de bewaartermijnen worden nageleefd. Gegevens zouden na de wettelijke bewaartermijn moeten worden verwijderd dan wel geanonimiseerd.

Tactieken:
- Mogelijkheid om de bewaartermijn per document in te regelen via retentielabels.
- Automatisch verwijderen van bepaalde gegevens op een vast moment, bijvoorbeeld einde schooljaar, al dan niet na handmatige bevestiging.
- Geef in back-ups een bewaarperiode mee aan bepaalde sleutels, zodat die data eenvoudig kan worden vernietigd door de sleutel te vernietigen.

Stap 8 – Faciliteer de rechten van betrokkenen

Zorg ervoor dat je mensen grip geeft op het gebruik van hun persoonsgegevens. Mensen hebben het recht op:

Inzage 

Verwijdering 

Beperking 

Correctie 

Bezwaar 

Overdracht 

Transparantie 

Tactieken:

- Een eigen account van de gebruiker waar men kan zien welke gegevens er zijn geregistreerd zijn, met de mogelijkheid deze te corrigeren en te verwijderen.
- Er zijn procedures om de rechten op inzage, verwijdering, beperking, correctie, bezwaar en overdracht te faciliteren.
- Mensen kunnen gemakkelijk achterhalen welke persoonsgegevens worden verwerkt en waarvoor dat is, bijvoorbeeld door met iconen te werken en de verwerkingen te publiceren. Er is makkelijk leesbaar beleid, bijvoorbeeld in de vorm van een privacyverklaring en privacyreglement en beleid. Het
- Mensen weten bij wie ze terecht kunnen met vragen.

Daarna: - Zorg voor management (technisch/functioneel)

Een programma dat eenmaal in gebruik is, moet worden onderhouden. Het technische stuk wordt verzorgd door de leverancier, die b.v. voorziet in updates/patches. De functioneel beheerder zorgt voor de benodigde technische ondersteuning van medewerkers binnen een bedrijf en zorgt ervoor dat de aanwezige applicaties functioneren en op correcte wijze gebruikt worden.

Een laatste stap in het beheer is een proces voor de uitfasering van een systeem/proces en de archivering van gegevens (zie ook stap 7). Zorg dat je weet hoe je die uitfasering aanpakt.

Tactieken:

- Maak afspraken met de leverancier in een SLA en controleer of die afspraken worden nageleefd.
- Als externe leveranciers het technisch beheer uitvoeren via een koppeling met hun eigen AD, heb je als organisatie geen grip op b.v. aantal accounts, veilig gebruik, (on)geoorloofde toegang. Het risico bestaat dat het geautoriseerde externe bedrijf zijn bevoorrechte toegang tot gegevens onrechtmatig gebruikt. Maak in zo'n situatie aanvullende afspraken over de toegang voor databasebeheertaken, zodat de veiligheid en rechtmatige toegang wordt gemonitord, bijvoorbeeld door logging en afspraken over de toegang (hoe vaak, een maximaal aantal accounts, het verwijderen van accounts als een medewerker van een leverancier uit dienst gaat, MFA en rapportage 1x per kwartaal.
- Maak een formeel proces waarin je de werkwijze voor de uitfasering van een systeem/proces beschrijft.

Bijlage 1 - Privacy by Design in de AVG (artikel 25)

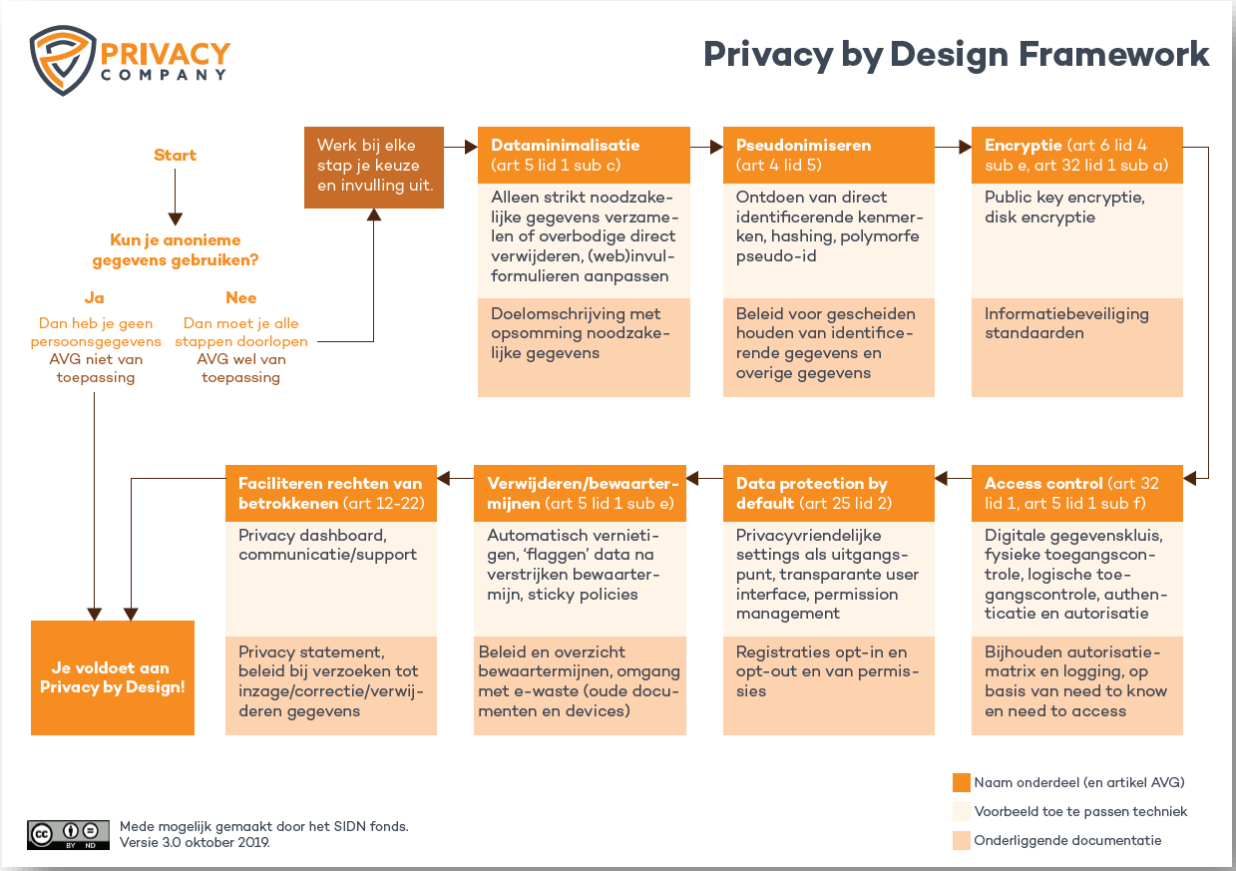
De verplichting om Privacy by Design toe te passen, volgt uit artikel 15 van de AVG:

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 die 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.*

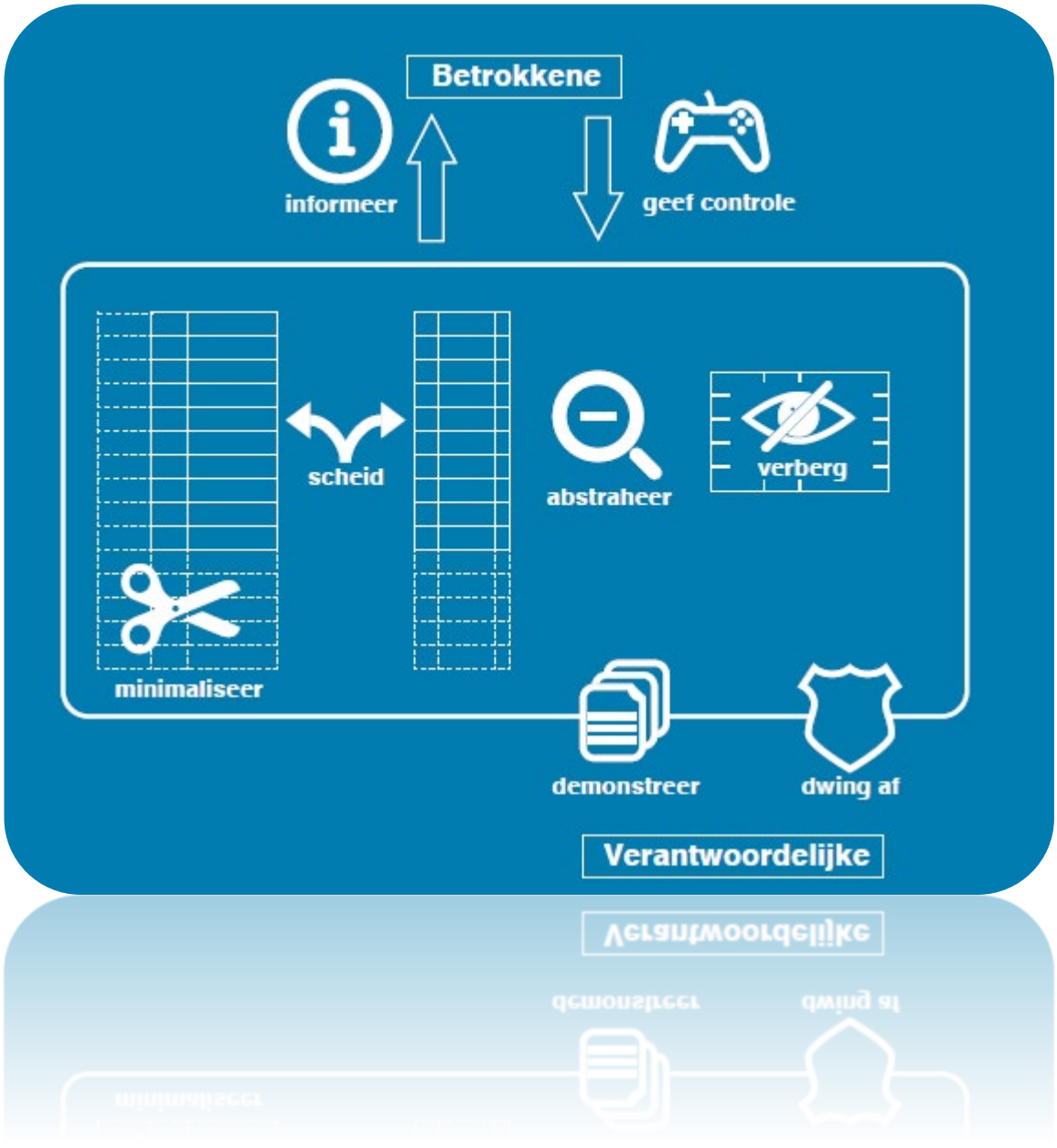
Bijlage 2 - Framework Privacy by Design (Privacy Company)

Deze basisprincipes voor Privacy by Design moeten in het framework landen.



Bijlage 3 – Technische en organisatorische maatregelen

In overzicht, naar Jaap-Henk Hoepman – binnen/in het vak: technische maatregelen, buiten het vak: organisatorische maatregelen:



Bijlage 4 – Verklarende woordenlijst

Betrokkene	Degene van wie persoonsgegevens worden verwerkt. Vaak een klant/eindgebruiker van een dienst of product.
Persoonsgegevens	Gegevens die direct of indirect herleidbaar zijn tot een (natuurlijk) persoon, zoals naam, pasfoto, geboortedatum, maar ook kenteken, postcode en IP-adres.
Privacy by Design	Ontwerpfilosofie die vereist dat privacybescherming vanaf het begin wordt meegenomen bij het ontwerpen en bouwen van nieuwe systemen.
Verantwoordelijke	Partij die bepaalt welke persoonsgegevens worden verwerkt, hoe dat moet worden gedaan en met welk doel.
Verwerken	Het op welke manier dan ook iets doen met persoonsgegevens, zoals verzamelen, opslaan, bekijken, bewaren, gebruiken, delen, veranderen, verrijken, verwijderen.
Verwerker	Partij die in opdracht en volgens instructie van de verantwoordelijke persoonsgegevens verwerkt.