PRIVACY BY DESIGN

7 FOUNDATIONAL PRINCIPLES

WHITEPAPER

# GDPR: PRIVACY BY DESIGN IN PRAKTIJK

**In de aanloop naar 25 mei 2018, de datum waar de GDPR uit de overgangsfase naar de 'handhavingsfase' gaat, is er al veel gepubliceerd. In deze whitepaper gaan we even helemaal terug naar de basis: de Architectuur.**

De GDPR verwacht dat bij de (her)ontwikkeling van systemen, producten of diensten in het ontwerp rekening wordt gehouden met het beschermen van de persoonsgegevens.

Dit verschilt fundamenteel met het 'Privacy by default' principe, waar bijvoorbeeld op basis van standaard instellingen binnen een applicatie de maximale privacy van een betrokkene(n) wordt gewaarborgd. Denk bijvoorbeeld aan actief gebruik van 'opt-in' buttons in plaats van 'opt-out', waarbij de keuze altijd bij de betrokkene gelaten wordt.

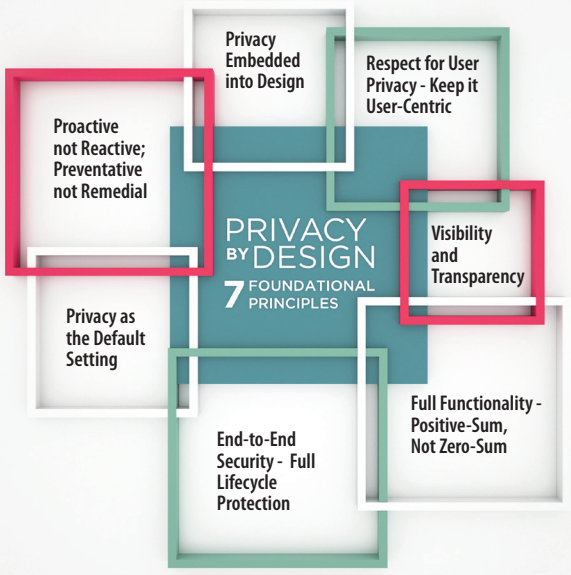
### De 7 principes

Ergens in de jaren '90 van de vorige eeuw bedacht Kim Cameron de '7 laws of Identity' die gebruikt zijn door Ann Cavoukian om de '7 foundational principles Privacy by Design' te ontwerpen. Nieuw is het dus zeker niet.

**Privacy by Design kan gezien worden als een set van architectuur principes die proactieve maatregelen in het ontwerp verwerken, in plaats van reactieve externe maatregelen buiten het ontwerp.**

Simpel gezegd, de applicatie, product of dienst heeft in de kern al bescherming van persoonsgegevens ingebouwd in plaats van een schil of lagen daaromheen die vaak technisch van aard zijn.

Het beperkt zich niet alleen tot de applicatie, product of dienst zelf, maar het omvat ook het beleid van de organisatie. En als dat nog niet het geval is, zouden de organisatie kernwaarden ook de privacy moeten omarmen.



**Twee principes uitgelicht**
Wat betekenen deze principes nu concreet? In deze whitepaper lichten we de twee belangrijkste toe, namelijk Privacy embedded into design en Visibility and transparency.

## Privacy embedded into design

De basis van dit principe is dat privacy een integraal onderdeel van het ontwerp is. Met andere woorden: privacy moet behandeld worden als een requirement net als alle andere functionele requirements van een oplossing.
Maar waar moet je dan precies aan denken?

### Data minimalisatie

Bij data minimalisatie moet er worden gewaarborgd dat er niet méér persoonsgegevens verwerkt worden dan strikt noodzakelijk is voor het doel van de verwerking.

*Voorbeeld:*
In het geval van een webshop is het vanzelfsprekend dat er naar naam en adres wordt gevraagd. Een geboortedatum of geboorteplaats is daarbij strikt gezien niet noodzakelijk. Tijdens het ontwerp zal er dus continue stil gestaan moeten worden welke persoonsgegevens noodzakelijk zijn en welke weggelaten kunnen worden.
Mocht er bijvoorbeeld om marketingdoeleinden wel behoefte zijn aan dit soort additionele persoonsgegevens (profilering), dan kun je dit vermelden en zorgen dat het een optioneel veld wordt. Hierbij past dan een duidelijke omschrijving van waar en hoe deze gegevens zullen worden gebruikt.

### Anonimiseren

Hier moet de vraag gesteld worden of het voor het product of de dienst noodzakelijk is om persoonsgegevens te verwerken of dat anonieme gegevens volstaan. Wanneer wel identificeerbase persoonsgegevens noodzakelijk zijn, is het van belang om na te denken over de beveiliging van deze gegevens.

*Voorbeeld*:
Stel dat we ooit een online kiessysteem krijgen, dan is het voor de validatie noodzakelijk om met direct identificeerbare persoonsgegevens toegang te krijgen. Het kiesresultaat zou dan niet samen met dit ID opgeslagen hoeven te worden, hooguit een geografisch kenmerk met een bijbehorend tijdstip.

## Visibility and transparency

Dit principe gaat over verantwoordelijkheid en vertrouwen: niet één van de makkelijke principes om te implementeren in het ontwerp.

In essentie kan dit principe opgedeeld worden in drie gebieden:

### Openheid

Openheid gaat over informatievoorziening. In het ontwerp moeten mogelijkheden worden opgenomen zodat de betrokkene informatie kan krijgen over bijvoorbeeld hoe de persoonsgegevens gebruikt worden, bewaartermijnen en verdere verwerking. In een applicatie zou dat bijvoorbeeld kunnen door een button met 'privacy transparantie'.

### Verantwoordelijkheid

Dit is naar alle waarschijnlijkheid de spil waar de GDPR echt om draait. Het is nu dan ook een onderdeel bij het ontwikkelen van een systeem, product of dienst.
Het is een nogal beladen term die in feite zegt dat je verantwoordelijkheid kan afleggen over hetgeen wat je gedaan en gezegd hebt. Dit moet dan meetbaar en toonbaar zijn.

*Voorbeeld*
Als we bijvoorbeeld persoonsgegevens verzamelen, opslaan en voor verwerking naar een derde partij doorzetten, dan zullen we er in het ontwerp voor moeten zorgen dat het transport en de beveiliging naar de systemen van de derde partij met de passende maatregelen zal gaan en dat dit gerapporteerd wordt. Met de bewerker zijn gelijkwaardige privacy afspraken gemaakt en de rapportage van ontvangst en verwerking wordt terug gestuurd aan het bron systeem. De betrokkene kan in duidelijke, leesbare rapportage inzicht krijgen waar en wanneer de persoonsgegevens zich bevinden en of alle bewerkingscontracten gevalideerd zijn.

### Compliance

Bij compliance is het noodzakelijk om in het ontwerp rekening te houden met monitoring, evalueren en het vergelijken met de huidige privacy richtlijnen en procedures. Op het moment dat een betrokkene het ergens fundamenteel mee oneens is, moet er de mogelijkheid zijn om dit direct kenbaar te maken. Denk hierbij aan een soort privacy feedback of een klachtenformulier.

Voor de monitoring, het evalueren en vergelijken zou het ontwerp bijvoorbeeld template- achtige policies kunnen bevatten, die als een schil over de gegevensverzameling geplaatst is en eenvoudig aangepast kan worden zonder de structuur van het ontwerp aan te passen.

Privacy by Design is niet alleen van belang voor de ontwerpers van een product of dienst. Alle lagen in een organisatie zullen over privacy en persoonsgegevens bescherming moeten nadenken zodat het als het ware in het DNA van de medewerker komt te zitten. Tenslotte is een medewerker bij het ene bedrijf een betrokkene bij een ander bedrijf.

Privacy by Design is een ingewikkeld en interessant onderdeel binnen een ontwerp. In de komende maanden zullen er zeker een aantal 'best practices of templates voor worden ontwikkeld.

## Bauhaus ArtITech & Privacy by Design

Als Bauhaus ArtITech blijven we inspelen op de laatste ontwikkelingen. Heb je vragen of wil je even sparren? Neem dan contact op met één van onze experts via telefoonnummer +31 30 711 88 44

*Auteur: Menno De Gans - Enterprise & Data Protection / Privacy Architect*

**Bauhaus ArtITech**
Van Deventerlaan 30 - 40
3528 AE Utrecht

Tel. +31 30 711 88 44
info@bauhaus.nl
www.bauhaus.nl