De link tussen 'design' en 'privacy'

In het vorige nummer van Product werd stilgestaan bij 'The Internet of Things', de ontwikkeling dat steeds meer gebruiksvoorwerpen worden voorzien van sensoren en continu gegevens uitwisselen met andere apparaten. Het dataprotectierecht komt hiermee de werkkamer van de ontwerper en productontwikkelaar binnen. En eigenlijk hoort het daar ook, vindt een toenemend aantal privacy experts.



Wat is Privacy by Design?

De term 'Privacy by Design' (PbD) is niet in de wet omschreven en kent geen algemeen aanvaarde definitie. Met de term wordt gewoonlijk gedoeld op het vanaf het eerste ontwikkelstadium van een informatiesysteem of een product meenemen van privacy principes, en het inbedden van maatregelen ter bescherming van de verwerkte persoonsgegevens. Het gaat daarbij niet alleen over techniek, maar ook over afspraken, (gebruiks)voorschriften en feedback binnen de organisatie over de verwerking van persoonsgegevens. Dit alles moet al in de ontwerpfase worden meegenomen: welke gegevens *kunnen* worden opgeslagen en welke gegevens *willen* we behouden?
TNO bracht in 2012 een rapport uit over PbD waarin drie categorieën PbD-principes worden genoemd. -1- al bij het (vroegste) ontwerp van een systeem rekening houden met de bescherming van de privacy van personen over wie gegevens worden verzameld (bijvoorbeeld de gebruikers van een apparaat of app). -2- het treffen van organisatorische maatregelen om toegang tot en omgang met persoonsgegevens te regelen volgens bepaalde afspraken en voorschriften. -3- toepassen van technische maatregelen om toegang tot en omgang met persoonsgegevens af te schermen of te verhinderen (bijvoorbeeld encryptie).

Verplichte kost

Op dit moment krijgt PbD vooral aandacht van onderzoekers en privacy-experts. De kans is groot dat dit gaat veranderen. In Brussel wordt hard gewerkt aan de goedkeuring van de Raad van Ministers voor de Algemene Verordening op de Gegevensbescherming (AVG). Deze nieuwe Europese privacywet is op 12 maart 2014 door het Europees Parlement goedgekeurd. De boetes die daarmee worden geïntroduceerd kunnen oplopen tot honderden miljoenen euro's. Daarnaast maakt de AVG werk van PbD. Artikel 23 bepaalt dat met de bescherming van persoonsgegevens rekening moet worden gehouden *"gedurende de hele levenscyclus van persoonsgegevens, vanaf het verzamelen tot het verwerken en verwijderen"* daarvan.

PbD en productontwikkeling

Een van de meest basale PbD-principes is gegevensminimalisatie: gegevens die niet worden opgeslagen kunnen ook niet verkeerd worden gebruikt. Maar ook door anonimisering of pseudonimisering en transparantie over het gebruik van gegevens kan de privacy van de gebruiker van een 'slim' product worden beschermd. Privacy by Design wordt daarom door velen gezien als toekomstig antwoord op de steeds verdergaande inbreuken op de privacy die gepaard gaan met moderne technologie.
Het toepassen van PbD in productontwikkeling betekent dus dat men zich al in het ontwerpstadium moet afvragen: *Welke gegevens kan dit product verzamelen? Is dat noodzakelijk voor het gebruiksnut? Weet de gebruiker welke gegevens worden verwerkt? Kan hij de gegevensverzameling stopzetten en de bewaarde gegevens laten verwijderen?*

Privacygevoelige bureaustoel

Stel dat een bureaustoel wordt voorzien van een sensor die de slijtage bijhoudt en waarschuwt wanneer de gasveer aan vervanging toe is. Die meetgegevens zouden informatie kunnen geven over de werktijden van de gebruiker, zijn bewegingspatroon, veranderingen in zijn gewicht, et cetera. De productontwikkelaar die de PbD-principes toepast, zorgt ervoor dat alleen de gegevens die nodig zijn om de slijtage te beoordelen worden verwerkt.
Alleen al door te zorgen dat geen tijdsinformatie wordt meegenomen, wordt de privacy van de bezitter van de stoel beschermd. Wanneer het systeem vervolgens zo wordt ingericht dat de gegevens slechts door de fabriek kunnen worden ontcijferd, wordt het nog moeilijker voor derden om (gevoelige) informatie te bemachtigen. Sluitstuk zou zijn dat de fabrikant afspraken maakt om de meetgegevens op een privacy-veilige manier te verwerken én de gebruikers inzicht geeft in het hoe en waarom van de gegevensverzameling. Privacy (by Design) is dus nu al een zaak voor de moderne productontwikkelaar en die trend zal nog lang doorzetten. «



Wouter Seinen is advocaat bij CMS in de praktijkgroep intellectuele eigendom, technologie, media en telecommunicatierecht (e-mail: wouter.seinen@cms-dsb.com)