PRIVACY BY DESIGN: U KUNT ER NIET OMHEEN

Het zal de lezer niet zijn ontgaan: de Algemene Verordening Gegevensbescherming (AVG) vervangt per 25 mei 2018 de bestaande Wet bescherming persoonsgegevens. Partijen die persoonsgegevens verwerken zullen hier rekening mee moeten houden. De AVG borduurt qua basisbeginselen voort op de bestaande regelgeving en introduceert nieuwe vereisten die in acht moeten worden genomen bij de verwerking van persoonsgegevens. Wij willen eens iets meer inzoomen op één noviteit van de AVG: de eis van privacy by design.

TEKST: **JAN BRÖLMANN** EN **JURRE REUS** BEELD: **SHUTTERSTOCK**

Jan Brölmann (boven) en **Jurre Reus** zijn beiden advocaat it- en privacyrecht bij Houthoff.

In de officiële toelichting bij de AVG staat: *When developing, designing, selecting and using applications, services and products (...), producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications (...).*
Kort gezegd dient bij de ontwikkeling van software, producten en diensten al rekening te worden gehouden met de bescherming van persoonsgegevens. Privacy by design is een term die al enige tijd bekend is in it- en privacyland, maar een specifieke wettelijke verplichting was er tot nog toe niet.
Allereerst is belangrijk om te verduidelijken is dat de AVG onderscheid maakt tussen een '(verwerkings)verantwoordelijke' en een 'verwerker'. Een verantwoordelijke is een partij die zelf bepaalt hoe en waarom persoonsgegevens worden verwerkt. Hij stelt de 'middelen' en 'doeleinden' vast. Een verwerker is een partij die ook persoonsgegevens verwerkt, maar dit uitsluitend doet op instructie van een verantwoordelijke. Simpel gezegd: hij mag niets met deze persoonsgegevens doen voor eigen doeleinden. In een ict-context is een verwerker vaak een ict-dienstverlener (hosting provider, SaaS-aanbieder) en is de verantwoordelijke zijn klant.
Privacy by design is gericht tot de verantwoordelijke. Vanuit een ict-perspectief betekent dit dat de klant (als verantwoordelijke) moet voldoen aan de verplichting van privacy by design. Als de klant een ict-dienstverlener (als verwerker) inschakelt, dan zal de klant ervoor moeten zorgen dat het afgenomen product of de afgenomen dienst voldoet aan het vereiste van privacy by design, ook al heeft de klant het product of de dienst niet zelf ontwikkeld. De klant verwerkt er immers persoonsgegevens mee.
Wat betekent dit nou concreet? De

AVG verplicht de verantwoordelijke om rekening te houden met privacy by design bij de ontwikkeling, de uitwerking, de keuze en het gebruik van toepassingen, diensten en producten. De verantwoordelijke moet dus maatregelen nemen. Hij kan dit bijvoorbeeld doen door intern beleid op te stellen, dataminimalisatie-technieken toe te passen, instellingen standaard op privacyvriendelijk (privacy by default) te zetten, in een vroeg stadium gegevens te pseudonimiseren, zodat deze moeilijker herleidbaar zijn tot iemand, en door mogelijkheden te bieden om (extra) transparant te zijn, bijvoorbeeld door mensen hun eigen gegevensgebruik te kunnen laten monitoren.
Onder de AVG hebben mensen nogal wat rechten die zij richting een verantwoordelijke kunnen inroepen. Denk aan inzage, correctie, rectificatie, dataportabiliteit (gegevens meenemen), 'vergeten worden' en het recht om een verwerking 'te beperken'. Het effectief en gebruiksvriendelijk aanbieden van mogelijkheden voor mensen om die rechten uit te oefenen wordt door privacy by design ook aangemoedigd.
Bij het toepassen van maatregelen gericht op privacy by design moet trouwens wel rekening worden gehouden met factoren die bepalen hoe ver de maatregelen moeten gaan (potentiële beperkingen dus): de stand van de techniek, uitvoeringskosten, de aard, omvang, context en het doel van de verwerking en *last but not least* de mogelijke uiteenlopende risico's van de verwerking.
Volgens de letter van de AVG geldt de verplichting van privacy by design alleen voor verantwoordelijken. Dat wil echter niet zeggen dat verwerkers hier geen rekening mee zouden moeten houden. Integendeel, de AVG is voor zowel verantwoordelijken als verwerkers relevant! Softwareontwikkelaars die een SaaS-applicatie ontwikkelen willen hun klant iets bieden dat voldoet aan de wettelijke vereisten. Als de applicatie het technisch maar ook organisatorisch (bedrijfsmatig, in de uitvoering) voor de klant niet mogelijk maakt om te voldoen aan de AVG, simpelweg omdat deze niet voldoet aan privacy by design, zal de klant een andere applicatie moeten kiezen. Softwaredevelopers, ict-dienstverleners en andere partijen die doorgaans als verwerker optreden voor klanten, zullen dus ook rekening moeten houden met privacy by design. U kunt er bij de verwerking van persoonsgegevens niet omheen! ◀