Jurel

Recht in de electronische en virtuele wereld

« Old, confusing ruling by EU court of Justice on general information requirement

CBP presenteert de richtsnoeren voor beveiliging van persoonsgegevens

De urgentie

De deskundigen hebben lang uitgekeken naar de opvattingen van het College voor de Bescherming van de Persoonsgegevens, omdat de beveiliging van persoonsgegevens hot is. Het digitaal werken kent zijn voordelen, maar ook zijn risico's. Denk niet alleen aan hacken, maar vooral aan onbewust en onzorgvuldig omgaan met data. Een inmiddels bekend voorbeeld is een gebrekkige front office applicatie, zodat ongewenste buitenstaanders toegang krijgen tot achterliggende back office applicaties plus databases, gevuld met bijvoorbeeld personeels- of cliëntgegevens.

De Europese wetgever heeft reeds in Richtlijn 95/46/EG regels gesteld ter zake van de verwerking van persoonsgegevens. Het belangrijke artikel 13 Wet bescherming persoonsgegevens (Wbp) legt in Nederland bedrijven en overheden de verplichting op ''passende technische en organisatorische maatregelen'' te treffen om persoonsgegevens te beveiligen. Het artikel geeft geen helderheid over de invulling van de genoemde verplichting. Daarom heeft het CBP de richtsnoeren voor beveiliging van persoonsgegevens deze week gepresenteerd.

Standaarden met open normen

Het college kiest voor de volgende benadering. Formuleer betrouwbaarheidseisen, gerelateerd aan de verschillende typen persoonsgegevens. Reken hiertoe beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid. Leg vervolgens de geformuleerde eisen ten grondslag aan de analyse van de risico's en de te treffen maatregelen. Evalueer de uitvoering van de maatregelen. Voor zover nodig stel de maatregelen bij.

De lezer van de CBP-Richtsnoeren krijgt dus geen inhoudelijke oplossingen gepresenteerd, maar een aanpak voor hoe om te gaan met informatiebeveiliging. Hierbij wordt verwezen naar de beschikbare standaarden. Reken hiertoe bijvoorbeeld de code voor informatiebeveiliging (NEN-ISO 2702:207) en de NEN 7510. Zoals bekend gaat het hier om open normen. De ''verantwoordelijke'' (lees : degene, die doel en middelen voor verwerking van persoonsgegevens vaststelt) en de ''bewerker'' (lees : verwerkt in opdracht van de verantwoordelijke) zullen dus zelf de risicoanalyse moeten maken en op basis hiervan de beveiligingsmaatregelen moeten formuleren. Een voorbeeld ter illustratie. De leverancier van medische apps heeft een zware zorgplicht met betrekking tot de patiëntgegevens die ontstaan en worden opgeslagen. De beveiliging daarvan zal op een 99.9%-niveau moeten plaats vinden. Lukt dat niet in 1 keer, dan moet de fasering met maatregelen SMART (Specifiek, Meetbaar, Aanvaardbaar, Realistisch en Tijdgebonden) zijn.

Een tweede constatering ter zake van de genoemde standaarden is dat zij het uiterlijk van zware kerstbomen hebben. Het is derhalve onmogelijk om alle beveiligingsmaatregelen tegelijkertijd uit te voeren. Dat leert ook de praktijk. Het stellen van prioriteiten (risico's en maatregelen in de tijd gefaseerd) moet derhalve gebaseerd zijn op een transparante en resultaatgerichte 'control approach''. Een praktische aanpak kan zijn de risico's en de maatregelen te inventariseren en te benoemen binnen de aandachtsgebieden van bedrijfsdoelstellingen, de inrichting van de organisatie (de bedrijfsprocessen en de functies) en de ICT-systemen. Daarmee wordt voor niet alleen het management, maar ook voor de

toezichthouders , de medewerkers en de andere stakeholders helder wat de betekenis van beveiliging binnen de organisatie is.

Toezicht op de naleving

De verantwoordelijke moet op grond van art.14 Wbp overeenkomsten met (sub) bewerkers afsluiten. Voor deze overeenkomsten geldt de plicht om per groep gegevens de beveiligingseisen vast te leggen. De risicoanalyse is dus van belang. Deze is tevens de opstap naar de te treffen maatregelen.

Het CBP stelt dat de naleving van de beveiligingseisen gewaarborgd moet zijn. De keuze voor welke control instrumenten zullen worden gehanteerd zal derhalve een plaats moeten krijgen in de bewerkersovereenkomst. Dit, met het oog op de beoordeling van de nakoming van de overeenkomst tussen verantwoordelijke en bewerker. Voorbeelden van control instrumenten zijn audits, penetratietesten, visitaties en zelfevaluaties. Het is cruciaal dat de control resultaten een plaats krijgen in rapportages passende binnen de reguliere planning- en controlcycli van organisaties. In geval van aanzienlijke veranderingen in de dienstverlening door bewerker en eventueel subbewerkers stelt de verantwoordelijke vast of de gemaakte afspraken nog toereikend zijn. Omgekeerd kunnen ook veranderingen in de bedrijfsvoering van de verantwoordelijke aanleiding geven tot wijzigingen in de afspraken.

Toezicht uitoefenen door het CBP op basis van onder andere de artikelen 12, 13 en 14 Wbp is een actieve bezigheid. Met behulp van het voeren van gespreken en de beschikking over de controlresultaten kan de toezichthouder beoordelen of passende beveiligingsmaatregelen zijn genomen en ook werken in de praktijk.

Constateringen

Naar onze mening zijn de richtsnoeren van het College een aanzet tot hoe om te gaan met het treffen van passende organisatorische en technische maatregelen op grond van art.13 Wbp. De betrouwbaarheidseisen met betrekking tot de relevante persoonsgegevens moeten zichtbaar worden. En er moet inzicht ontstaan in de risico's en de maatregelen. De weg daarnaar toe is in beginsel vrij en dus naar eigen inzicht. Zoals bekend groeien de bomen in Nederland en in Europa niet meer tot in de hemel. Iedereen moet rekening houden met afnemende budgetten. Zou de wetgever bij het schrijven van art.13 Wbp zich dat ook al gerealiseerd hebben? De maatregelen , die een passend beveiligingsniveau waarborgen in relatie met de risico's, houden rekening met de stand der techniek en de kosten van tenuitvoerlegging.

Kees Zwinkels en Willem Balfoort (De Clercq Advocaten en Notarissen)

Leave a Reply

Name (required)

Mail (will not be published) (required)

Website

Submit Comment

Jurel is proudly powered by WordPress
Entries (RSS) and Comments (RSS).