CBP Richtsnoeren

BEVEILIGING VAN PERSOONSGEGEVENS

SAMENVATTING

Verantwoord omgaan met persoonsgegevens valt of staat met een adequate beveiliging van de gegevens. In de praktijk blijkt dat de aandacht voor beveiliging nogal eens tekortschiet. In de media zijn vrijwel dagelijks berichten te vinden over datalekken door onvoldoende beveiliging, waardoor persoonsgegevens op straat liggen. Het College bescherming persoonsgegevens (CBP) ontvangt ook regelmatig signalen over tekortschietende beveiliging en de kwalijke gevolgen ervan.

Beveiliging van persoonsgegevens is een van de speerpunten van het handhavingsbeleid van het CBP. Het CBP houdt toezicht op de naleving van de Wet bescherming persoonsgegevens (Wbp). Artikel 13 van de Wbp eist dat bedrijven en overheden die persoonsgegevens verwerken, 'passende technische en organisatorische maatregelen' nemen om persoonsgegevens te beveiligen.

Voldoen aan de wettelijke normen
Wanneer zijn beveiligingsmaatregelen nu 'passend' zoals de Wbp eist? Deze richtsnoeren leggen uit hoe het CBP bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens in individuele gevallen de beveiligingsnormen uit de Wbp toepast. De richtsnoeren vormen de verbindende schakel tussen enerzijds het juridisch domein, met daarbinnen de eisen uit de Wbp, en anderzijds het domein van de informatiebeveiliging, waarin de noodzakelijke kennis en kunde aanwezig is om daadwerkelijk aan die eisen te voldoen.

Dat betekent dat de richtsnoeren in samenhang moeten worden gebruikt met algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van de informatiebeveiliging, zoals de Code voor Informatiebeveiliging of de ICT-beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum.

Op tijd beginnen
Het uitgangspunt om tot een passende beveiliging te komen is dat in een organisatie bestuurders en de mensen die verantwoordelijk zijn voor de informatiesystemen en -beveiliging gezamenlijk nadenken over de wijze van beveiliging, al vóórdat ze persoonsgegevens gaan verzamelen. De beveiliging van persoonsgegevens binnen een organisatie moet gedurende de gehele levensduur van een informatiesysteem punt van aandacht zijn, van het allereerste ontwerp tot aan het onomkeerbaar wissen van het laatste back-up-bestand na afloop van de bewaartermijn. De beveiliging past binnen het bredere verband van *privacy by design*, waarbij de bescherming van persoonsgegevens en de borging van de rechten van de betrokkenen vanaf het allereerste begin in de informatiesystemen wordt ingebouwd.

'Plan-do-check-act'
Voor een blijvend passend beveiligingsniveau is inbedding van de zogeheten plan-do-check-act-cyclus in de dagelijkse praktijk van de organisatie noodzakelijk. Dat komt kort gezegd op het volgende neer:

1. *Beoordeel de risico's*
   Beoordeel de risico's die de gegevens en de aard van de verwerking met zich meebrengen voor de betrokkenen en bepaal op basis daarvan het gewenste beveiligingsniveau. Inventariseer vervolgens de dreigingen die kunnen leiden tot een beveiligingsincident, de gevolgen die het beveiligingsincident kan hebben en de kans dat deze gevolgen zich voor zullen doen. Tref op basis daarvan gericht beveiligingsmaatregelen die het gewenste beveiligingsniveau kunnen waarborgen.
2. *Maak gebruik van algemeen geaccepteerde beveiligingsstandaarden*
   Het vakgebied informatiebeveiliging kent vele beveiligingsmethoden, -standaarden en -maatregelen die zijn gebaseerd op ervaringen uit de dagelijkse beveiligingspraktijk. Gebruik bij het nemen van beveiligingsmaatregelen de richtsnoeren in samenhang met de beschikbare beveiligingsstandaarden. Deze standaarden geven houvast bij het daadwerkelijk treffen van passende maatregelen om de beveiligingsrisico's af te dekken.
3. *Controleer en evalueer regelmatig*
   Controleer met zekere regelmaat of de beveiligingsmaatregelen daadwerkelijk zijn getroffen en worden nageleefd. Beoordeel periodiek of het beveiligingsniveau nog steeds past bij de risico's die de verwerking en de aard van de te verwerken gegevens met zich meebrengen en of de beveiligingsmaatregelen nog steeds voldoen. Betrek daarbij ook de stand van de techniek en de nieuwste inzichten binnen het vakgebied informatiebeveiliging. Pas waar nodig de beveiligingsmaatregelen aan.

Tot slot

Met deze richtsnoeren wil het CBP duidelijk maken wat het van de beveiliging van persoonsgegevens verwacht. Daarbij heeft een organisatie de ruimte om de beveiliging van persoonsgegevens in te richten op de wijze en met de middelen die in de specifieke situatie van deze organisatie het meest passend zijn. Een organisatie dient hierbij altijd de rechten van de betrokkenen te waarborgen en er moet sprake zijn van adequate, vakkundig toegepaste beveiliging waarbij de organisatie optimaal benut wat het vakgebied informatiebeveiliging te bieden heeft.