INFORMATIE
BEVEILIGINGS
DIENST

MELDPLICHT DATALEKKEN

De Meldplicht Datalekken is geïntroduceerd in een wetsvoorstel als aanvulling op de Wet bescherming persoonsgegevens (Wpb). In februari 2015 is dit voorstel met algemene stemmen door de Tweede Kamer aangenomen. Dit wetsvoorstel voegt aan de Wbp een meldplicht voor inbreuken op beveiligingsmaatregelen voor persoonsgegevens toe. Deze factsheet biedt extra achtergrondinformatie over het wetsvoorstel en geeft onder andere antwoord op vragen als 'Wat houdt de Meldplicht Datalekken in?', 'Wanneer moet ik melding doen?' en 'Wie is aansprakelijk?'.

WAT HOUDT DE MELDPLICHT DATALEKKEN IN?

Met de Meldplicht Datalekken wil de regering de gevolgen van een datalek voor de betrokkenen zoveel mogelijk beperken en hiermee een bijdrage leveren aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens. Met dit voorstel moet de verantwoordelijke bij een datalek, waarbij kans is op verlies of onrechtmatige verwerking van persoonsgegevens, niet alleen een melding doen bij de toezichthouder, het College Bescherming Persoonsgegevens (CBP), maar ook de betrokkene informeren. Als er geen melding wordt gemaakt van een datalek kan dit bestraft worden met een bestuurlijke boete van het CBP. Op Europees niveau wordt eveneens gewerkt aan een wijziging van een wettelijk kader dat de privacyrichtlijn moet gaan vervangen. Ook daarin komt de Meldplicht Datalekken aan de orde.

IMPACT VOOR GEMEENTEN

Door verschillende landelijke ontwikkelingen komt er een groeiende hoeveelheid privacygevoelige informatie bij gemeenten te liggen. De Meldplicht Datalekken heeft daarom zeker ook impact op uw gemeente. Zo zal het CBP onder andere onderzoek doen naar de beveiliging van persoonsgegevens en worden maatregelen getroffen om de meldingen op een efficiënte en effectieve manier te verwerken.

WAT IS EEN DATALEK EN WANNEER MOET IK MELDING DOEN?

Wanneer technische en organisatorische beveiligings-maatregelen niet hebben gefunctioneerd, dient u hiervan melding te doen. Persoonsgegevens zijn dan blootgesteld aan een aanmerkelijke kans op onbedoelde of onwettige vernietiging, verlies of onrechtmatige wijziging van, of een niet geautoriseerde toegang tot persoonsgegevens. Het moet gaan om 'ernstige' nadelige gevolgen voor de betrokkene. De aard en omvang van het lekken speelt hierbij dus een belangrijke rol.

Een inbreuk op de beveiliging hoeft niet te betekenen dat beveiligingsmaatregelen niet voldoende zijn. Gegevens kunnen bijvoorbeeld ook in verkeerde handen zijn gevallen door bijvoorbeeld diefstal van een computer, laptop of tablet. Het kan ook gaan om menselijke fouten; denk bijvoorbeeld aan het verzenden van gevoelige gegevens naar een onjuist e-mailadres zonder versleuteling. In al deze gevallen dient u bij het CBP melding te doen van een datalek.

"BIJ TWIJFEL, MELD DATALEKKEN ALTIJD BIJ DE IBD"

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

U hoeft geen melding te doen wanneer u kunt aantonen dat er gepaste technische beschermingsmaatregelen zijn genomen, zoals versleuteling van de gegevens of andere technieken die persoonsgegevens ontoegankelijk kunnen maken wanneer een datalek plaatsvindt. Denk bijvoorbeeld aan een 'remote wipe' op een smartphone of tablet. Het CBP kan in sommige gevallen besluiten dat er toch een melding moet worden gedaan aan de betrokkene als blijkt dat de versleuteling omzeild zou kunnen worden of te zwak is.

WIE IS AANSPRAKELIJK?

De bestuurder van een gemeente is aansprakelijk voor de eventuele schade die ontstaat bij een datalek en dient hiervan melding te doen bij het CBP. Tevens dient er een administratie bijgehouden te worden met betrekking tot de datalekken.

In het wetsvoorstel 'Meldplicht Datalekken' is nog geen termijn benoemd waarbinnen een datalek gemeld moet zijn. Ook de definiëring van 'ernstig' en de beleidsregels dient het CBP nog op te stellen.

WAT MOET HET CBP WETEN?

Wat moet je als gemeente aan het CBP kunnen melden als er een 'ernstig' datalek is geconstateerd:

- de aard van de inbreuk
- de namen van instanties die meer informatie over de inbreuk kunnen geven
- de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken
- een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens
- de maatregelen die de gemeente heeft genomen of voorstelt te nemen om deze gevolgen te verhelpen

MELDEN BIJ BETROKKENE

Als er een datalek is geconstateerd met aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, dan moet de betrokkene daar ook van in kennis worden gesteld. Op dit moment is er nog geen definitie van 'aanzienlijke kans op ernstige gevolgen…' dus dat blijft een afweging van de verantwoordelijke op basis van de aard van het datalek, de gevolgen voor de betrokkene(n) en kosten van de uitvoering. Ook hier dient een registratie van bijgehouden te worden.

CONCRETE TIPS

Om goed voorbereid te zijn op de aanstaande wetswijziging geeft de IBD graag een aantal tips. Deze tips hangen nauw samen met de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

- Er moet achteraf aantoonbaar op basis van een risicoafweging zijn nagedacht over de privacy en passende informatiebeveiliging. Een manier om dit te kunnen aantonen is dat een baselinetoets wordt uitgevoerd, eventueel gevolgd door een risicoanalyse, een Privacy Impact Assessment (PIA) en implementatie van de maatregelen. De basismaatregelen in de BIG zijn veelal passend tenzij er bijzondere persoonsgegevens worden verwerkt.
- Documenteer; zonder documentatie is er geen compliance.
- Benoem verantwoordelijken en hun verantwoordelijkheden in het gemeentelijk beveiligingsbeleid, bijvoorbeeld een Chief Information Security Officer (CISO) of een functionaris gegevensbescherming.
- Draag zorg voor encryptie van persoonsgegevens om te voorkomen dat bij een datalek de gegevens kunnen worden gelezen door een derde. Dit geldt voor persoonsgegevens in transport en in opslag.
- Richt een incidentmanagementproces in om ervoor te zorgen dat bij incidenten tijdig en doeltreffend kan worden gehandeld.
- Registreer alle gegevensverzamelingen en vermeld wat er met betrekking tot informatiebeveiliging is gedaan. Zorg voor passende procedures en technische maatregelen om een datalek te kunnen ontdekken, denk hier aan de incidentprocedure, logging en monitoring en analyseren van de logging.
- Zorg voor bewustwording bij medewerkers. Ook zij dienen te weten wat datalekken zijn, hoe de incidentprocedure werkt en wat de gevolgen kunnen zijn van een datalek voor de gemeente.

VOORTGANG VOORSTEL WETSWIJZIGING

De voortgang over de wetswijziging met betrekking tot de Meldplicht Datalekken is te volgen op de website van de Eerste Kamer. Uiteraard volgt de IBD de ontwikkelingen op de voet. Relevante nieuwsberichten hierover zijn ook te vinden op www.IBDgemeenten.nl.

MEER INFORMATIE

MEER INFORMATIE OVER ONZE DIENSTVERLENING VINDT U IN DE ANDERE FACTSHEETS VAN DE IBD EN OP DE WEBSITE WWW.IBDGEMEENTEN.NL. HIER KUNNEN GEMEENTEN BOVENDIEN VIA DE COMMUNITY RELEVANTE INFORMATIE MET ELKAAR DELEN, VRAGEN AAN ELKAAR STELLEN EN DOCUMENTEN UITWISSELEN. DE HELPDESK VAN DE IBD IS TE BEREIKEN TIJDENS KANTOORUREN VAN 9:00 TOT 17:00 UUR OP HET NUMMER 070 373 8011 OF VIA HET E-MAILADRES INFO@IBDGEMEENTEN.NL. TIJDENS DEZE KANTOORUREN REAGEERT DE IBD BINNEN 30 MINUTEN OP EEN INCIDENTMELDING. BUITEN KANTOORUREN IS DE IBD OP HETZELFDE NUMMER BEREIKBAAR VOOR SPOEDEISENDE MELDINGEN EN ZAL DE IBD BINNEN 60 MINUTEN REAGEREN OP EEN TELEFONISCHE OPROEP.