ZANDVOORT LEGAL
Jouw advocaten en juristen

WHITEPAPER

Meldplicht datalekken, weet jij wat je moet doen?

Door: Team Zandvoort Legal

MELDPLICHT DATALEKKEN, WEET JIJ WAT JE MOET DOEN?

Met dit stappenplan en deze tips rondom datalekken, voorkom je hoge boetes van de autoriteit persoonsgegevens!

Veel mensen werken thuis tijdens de coronacrisis. Dit brengt weer nieuwe uitdagingen met zich mee die ontstaan als gevolg van het online werken en vergaderen. Het risico hiervan is dat de beveiliging misschien minder goed op orde is dan op het werk zelf. Hierdoor kunnen gevoelige gegevens op straat komen te liggen. Juist in deze "thuiswerk tijd" is het dus extra van belang dat je op de hoogte bent van de risico's van datalekken. En vooral welke stappen je moet ondernemen indien er sprake is van een dergelijk datalek.

In deze Whitepaper leg ik uit wat een datalek is, wanneer deze gemeld moet worden aan de Autoriteit Persoonsgegevens en/ of aan de betrokkene(n) en hoe je met dit probleem moet omgaan in de praktijk. Daarbij voorzie ik je van een stappenplan en een aantal tips.

Onderwerpen in dit whitepaper:

MELDPLICHT DATALEKKEN,
WEET JIJ WAT JE MOET DOEN?

Inleiding

Dat bedrijven voorzichtig moeten omgaan met gegevens van personen is niet nieuw. In de AVG is een verplichting opgenomen, waarin staat dat een inbreuk in verband met persoonsgegevens (een datalek) onder omstandigheden medegedeeld moet worden aan de Autoriteit Persoonsgegevens (AP) en soms ook aan de betrokkene.

Het doel van de meldplicht is om tot een betere bescherming van persoonsgegevens te komen. Wanneer persoonsgegevens onvoldoende zijn beschermd kan dit grote gevolgen hebben voor de betrokken persoon. Het is dan ook van belang, dat indien jij binnen jouw bedrijf een datalek ontdekt, jij daarop tijdig en passend handelt. De verplichte mededeling aan de Autoriteit Persoonsgegevens en in sommige gevallen aan de betrokkene is daar een uitwerking van.

De Autoriteit Persoonsgegevens houdt toezicht op de naleving van deze meldplicht. Voldoe jij als ondernemer niet aan de meldplicht wanneer er sprake is van een datalek, dan kan de Autoriteit Persoonsgegevens dit bestraffen met een bestuurlijke boete.

De boete kan maximaal € 20.000.000,00 of maximaal 4% van de wereldwijde jaaromzet van de onderneming bedragen. Zo heeft de Belastingdienst in 2021 een boete van € 2,75 miljoen opgelegd gekregen en Transavia een boete van € 400.000,00 voor de slechte beveiliging van persoonsgegevens. Booking.com kreeg een boete opgelegd van € 475.000,00 voor het te laat melden van een datalek. Hoe gaat jouw onderneming om met persoonsgegevens? Hoe ga je om met een datalek? Onder welke omstandigheden moet jij melding maken van een datalek? En hoe voorkom je (hoge) boetes van de Autoriteit Persoonsgegevens? In dit whitepaper praat ik je graag bij. Datalekken zijn namelijk niet te voorkomen, de boetes van de Autoriteit Persoonsgegevens wel!

ONDERWERP 1

Wat is een datalek?

Laten we beginnen bij het begin: wat valt er nu precies onder een datalek? Bij een datalek gaat het in principe om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is van deze organisatie. Dit kan zich op verschillende manieren uiten. Hieronder geef ik enkele voorbeelden:

- Het verlies van een laptop met klantgegevens;
- Het verlies van een USB-stick met niet-versleutelde persoonsgegevens;
- Een cyberaanval waarbij persoonsgegevens zijn toegeëigend;
- Persoonsgegevens zijn onbedoeld vernietigd, gewijzigd of vrij gekomen;
- Een besmetting met ransomware waarbij persoonsgegevens ontoegankelijk zijn gemaakt;
- Een hacker heeft toegang gekregen tot databestanden waarin persoonsgegevens zijn opgeslagen;
- Een calamiteit zoals een brand in een datacentrum;
- Het sturen van een e-mail naar een verkeerde persoon waarin persoonsgegevens van een ander staan vermeld.

Bij datalekken is sprake van een inbreuk op de beveiliging van persoonsgegevens. Bij een datalek zijn de persoonsgegevens dus verloren gegaan of onrechtmatig verwerkt. De beveiligingsmaatregelen van jouw onderneming hadden hier bescherming tegen moeten bieden. De Algemene verordening gegevensbescherming (AVG) geeft aan dat een persoonsgegeven alle informatie is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is.

ONDERWERP 2

Wanneer moet een datalek worden gemeld aan de autoriteit persoonsgegevens?

De meldplicht datalekken houdt in dat organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. In sommige gevallen moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

Of je een datalek moet melden, is afhankelijk van de (potentiële) impact van het datalek op de bescherming van persoonsgegevens en de persoonlijke levenssfeer van de betrokkenen. In beginsel moet je een datalek aan de Autoriteit Persoonsgegevens melden, tenzij het onwaarschijnlijk is dat ze een risico inhouden voor de rechten en vrijheden van betrokkenen. Twijfel je of hiervan sprake is? Leg jouw situatie dan aan ons voor zodat wij hierover een beoordeling kunnen maken.

Mocht je verplicht zijn een datalek te melden aan de Autoriteit Persoonsgegevens, dan dien je dit binnen 72 uur te doen. Wanneer je dat niet doet ben je waarschijnlijk in overtreding. Wanneer je te laat bent moet je dit motiveren. Alleen in uitzonderlijke gevallen accepteert de Autoriteit Persoonsgegevens een vertraagde melding na 72 uur. Organisaties kunnen een datalek melden via een webformulier van het Meldloket datalekken van de Autoriteit Persoonsgegevens. Zie: https://datalekken.autoriteitpersoonsgegevens.nl/.
Let wel op: een datalek moet altijd worden gedocumenteerd in je interne datalek register! Dus zelfs als je het datalek niet hoeft te melden aan de Autoriteit Persoonsgegevens, moet je het wel documenteren. Elke organisatie die verwerkingsverantwoordelijke is, moet volgens de privacywet een datalekregister opstellen. Hierin houd je bij welke datalekken er in jouw organisatie zijn geweest, zodat je kan leren van eerdere datalekken en maatregelen neemt om de kans op nieuwe datalekken te verminderen. Daarnaast dient het als bewijs naar de Autoriteit Persoonsgegeven dat je je houdt aan de meldplicht datalekken. Indien je een voorbeeld wenst te ontvangen van een datalekkenregister, kun je ons benaderen via het mailadres onderaan dit whitepaper.

ONDERWERP 3

Wanneer moet een datalek worden gemeld aan de betrokkene(n)?

Je hoeft de betrokkene(n) alleen te informeren als een datalek waarschijnlijk een hoog risico voor hun rechten en vrijheden oplevert. Als dat niet zo is, dan hoef je het datalek niet aan de betrokkene(n) te melden. Zorg er wel voor dat als jij het standpunt inneemt dat het datalek geen hoog risico oplevert voor de betrokkene(n), je aannemelijk moet kunnen maken dat er geen sprake is van een hoog risico. Het hoge risico bestaat niet meer wanneer er

bijvoorbeeld passende technische en organisatorische beschermingsmaatregelen zijn genomen, of wanneer achteraf maatregelen zijn genomen die de risico's voor de betrokkene hebben weggenomen. Om te bepalen of een datalek een hoog risico oplevert voor de betrokkenen, moet je onder andere kijken of het datalek kan leiden tot fysieke, materiële of immateriële schade voor de betrokkenen. Denk hierbij aan: discriminatie, (identiteits-)fraude, financiële schade of reputatieschade. Of hiervan sprake is, blijft natuurlijk afhankelijk van de omstandigheden van het geval. Ook hier geldt weer: twijfel je of sprake is van een meldplicht aan de betrokkene(n)? Leg jouw situatie dan aan ons voor zodat wij hierover een beoordeling kunnen maken.
De volgende punten zullen wij hierbij afwegen:

- De aard van de inbreuk
- De aard, gevoeligheid en de omvang van de persoonsgegevens
- De ernst van de gevolgen voor personen
- Het aantal getroffen personen
- Bijzondere kenmerken van de persoon
- Bijzondere kenmerken van jouw onderneming
- Etc.

ONDERWERP 4

Hoe moet dit worden vormgegeven in de praktijk?

Als er sprake is van een datalek, dan is het allereerst belangrijk dat de werknemer die een (mogelijk) datalek constateert dit incident onmiddellijk meldt bij de verantwoordelijke. De verantwoordelijke kan dan de afhandeling van het datalek oppakken en schadebeperkend handelen. De melding van het datalek aan de Autoriteit Persoonsgegevens dient binnen 72 uur te zijn gedaan. Het is daarom van belang dat binnen de organisatie bekend is wie de verantwoordelijke is, zodat medewerkers direct een melding kunnen doen. De verantwoordelijke kan vervolgens de aard en de ernst van het datalek in kaart brengen en beoordelen welke vervolgstappen genomen dienen te worden. Via het mailadres onderaan dit whitepaper kun je een voorbeeld van een protocol datalekken bij ons opvragen. Op deze wijze kun jij als werkgever het (al dan niet) melden van een datalek binnen je onderneming stroomlijnen en centraliseren, zodat er tijdig actie kan worden ondernomen!

Wanneer er sprake is van een datalek adviseer ik om je aan onderstaand stappenplan te houden:

1. **Zorg voor overzicht**
   Analyseer de volgende punten:
   - Wat is de aard van het datalek?
   - Gaat het om gelekte, vernietigde of gewijzigde gegevens?
   - Wat is de omvang van het lek?
   - Wie hebben er nu toegang (gehad) tot de gegevens?

2. **Handel schadebeperkend**
   Welke maatregelen kunnen worden genomen om het datalek te beëindigen dan wel te beperken?
   Enkele voorbeelden zijn:
   - Het op afstand wissen of versleutelen van gegevens op een gesloten laptop, tablet of smartphone.
   - Een gepubliceerd bestand offline halen
   - Een verkeerde ontvanger vragen om de gegevens te wissen

3. **Beoordeel of het waarschijnlijk is dat het datalek een risico oplevert voor de rechten en vrijheden van de betrokken personen.**

4. **Indien dit het geval is, zorg er dan voor dat je het datalek binnen 72 uur bij de Autoriteit Persoonsgegevens meldt.**

5. **Beoordeel of er sprake is van een hoog risico voor de rechten en vrijheden van de betrokken personen.**

6. **Indien dit het geval is, zorg er dan voor dat je het datalek meldt aan de betrokken personen.**

7. **Registreer het datalek in je verplichte interne datalekregister.**
   Het maakt hierbij niet uit of het datalek gemeld moest worden aan de Autoriteit Persoonsgegevens of niet. Elk datalek, ongeacht de aard en omvang hiervan, moet in je datalekregister worden geregistreerd.

Verder heb ik nog een paar algemene tips om te voorkomen dat jij te maken krijgt met een datalek:

- Verzamel geen (gevoelige) informatie die je niet nodig hebt.
- Verwijder (gevoelige) gegevens die je niet meer nodig hebt.

- Vergroot bewustwording onder je werknemers (door onder andere het hanteren van een protocol). Een privacyprotocol kunnen wij naar wens voor je opstellen.
- Vermijd openbare netwerken.
- Versleutel gevoelige data.
- Investeer in ICT-beveiliging.
- Wissel gevoelige gegevens op een veilige manier uit.
- Zorg voor een goede beveiligde omgeving in het geval van thuiswerken.
- Wees voorzichtig met het gebruik van cloud-, opslag- of e-maildiensten, zeker wanneer deze gratis zijn.
- Update software en apparaten tijdig.
- Gebruik veilige wachtwoorden en zo nodig een wachtwoordmanager.
- Houd werk en privé gescheiden.
- Wissel gevoelige gegevens op een veilige manier uit (bijv. met een wachtwoord of via Zivver).
- Vergrendel je computer of laptop als je van je plaats gaat en berg deze buiten werktijd veilig op.
- Wees alert op phisingmails.
- Download geen onbekende software.
- Zorg voor back-ups.

TOCH SPRAKE VAN EEN DATALEK?

Onderneem tijdig actie!

Twijfel je hoe je moet handelen? Wij helpen je graag met al je vragen omtrent dit onderwerp.

0412 - 649109 >

info@zandvoort-legal.nl >

ZET DIE EERSTE STAP

Toe aan een rechterhand?

Graag plannen we een afspraak om te kijken welke SamenwerkingsVorm past.

Neem contact op >

Auteur
Team Zandvoort Legal

E info@zandvoort-legal.nl

Bram van den Berghstraat 22
5348 JT Oss
Postbus 414, 5340 AK Oss

T (0412) 64 91 09
F (0412) 64 91 02
www.zandvoort-legal.nl

De rechterhand voor ondernemend Nederland.