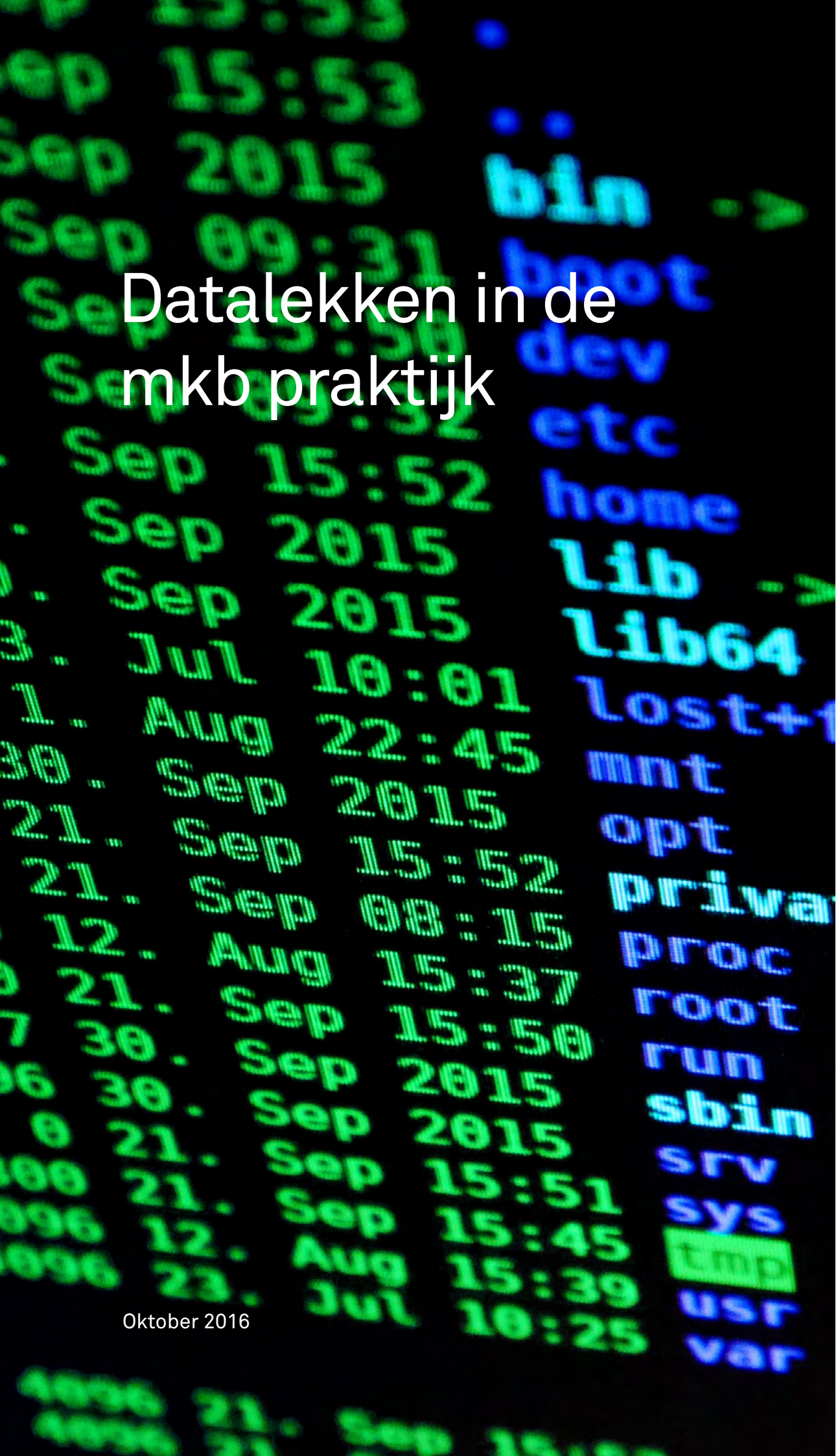

Datalekken in de mkb praktijk

Oktober 2016

MKB accountant

NBA

Disclaimer

Deze brochure is zo zorgvuldig mogelijk samengesteld. De NBA is echter niet aansprakelijk voor eventuele onjuistheden. De NBA heeft er voor gekozen een maximaal leesbare brochure op te stellen. Daarom zijn alleen de hoofdlijnen over het melden datalekken opgenomen. Voor een goede toepassing van de regelgeving is het noodzakelijk dat de wettelijke artikelen worden geraadpleegd. U vindt de artikelen in de Wet Bescherming Persoonsgegevens.

We hebben diverse voorbeelden *cursief* opgenomen. Deze voorbeelden zijn niet uitputtend.

Oktober 2016

Datalekken in de mkb praktijk

Sinds 1 januari 2016 zijn organisaties verplicht datalekken te melden bij de Autoriteit Persoonsgegevens. Soms moet het datalek ook gemeld worden aan betrokkene(n). Er moet dan sprake zijn van een datalek dat waarschijnlijk ernstige gevolgen heeft voor de persoonlijke levenssfeer van betrokkene(n). Deze verplichting heeft invloed op het werk van accountantskantoren en hun cliënten.

Wat moet ik geregeld hebben?

Overeenkomsten

Wanneer u bewerker bent moet de verantwoordelijke een overeenkomst met u gesloten hebben. Op uw beurt moet u eventueel weer overeenkomsten hebben met mogelijke subbewerkers.
Voorbeelden zijn op de NBA site (www.nba.nl) te vinden

Technische maatregelen

Om datalekken zo veel mogelijk te voorkomen moeten de verantwoordelijke en de (sub)bewerker passende maatregelen hebben genomen. Hierbij moet rekening worden gehouden met de stand van de techniek, het te beschermen belang en de kosten van de maatregelen. Dit moet leiden tot een beveiligingsniveau dat past bij de mogelijke risico's.
Er mag verwacht worden dat laptops, tablets en usb sticks die naar buiten gaan niet zo maar onbevoegd te gebruiken zijn. Ook moet een inlog-mogelijkheid via een portal professioneel zijn beveiligd.

Organisatorische maatregelen

Het spreekt voor zich dat personen die betrokken zijn bij het verwerken van persoonsgegevens voldoende kennis van de Wet Bescherming Persoonsgegevens hebben. Zij moeten een datalek herkennen en naar bevind van zaken handelen, zodat de schade beperkt blijft. Ook moeten er maatregelen genomen zijn die voorkomen dat er onnodige gegevensverzameling of –verwerking plaatsvindt.
Het naar een verkeerd adres sturen van documenten zal direct intern gemeld moeten worden, zodat de organisatie kan vaststellen of er een datalek heeft plaatsgevonden.
De medewerkers van de loonadministratie zullen instructies hebben over het verwijderen van loonbestanden na het verstrijken van de wettelijke bewaartermijn.

Wanneer moet ik een datalek melden en waar doe ik dat?

Te melden datalek

Niet ieder beveiligingsincident is een datalek en niet ieder datalek is zo ernstig dat het moet worden gemeld. Melden is verplicht als de aard en omvang van de inbreuk een grote kans op nadelige gevolgen heeft voor de bescherming van de verwerkte persoonsgegevens.
Het per abuis mailen van de loonstroken naar een verkeerd mailadres moet gemeld worden.

Bij wie meld ik en wanneer?

Het is de verantwoordelijke die een datalek onverwijld aan de Autoriteit Persoonsgegevens moet melden. In het algemeen

betekent onverwijld: binnen 72 uur na het ontdekken.
Het melden kan via: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

Verantwoordelijke en bewerker kunnen afspreken dat de bewerker de melding namens de verantwoordelijke doet. Met de subbewerker moeten goede afspraken worden gemaakt over melding van een eventueel datalek aan de bewerker of rechtstreeks aan de verantwoordelijke. Gezien de verplichting om in ieder geval binnen 72 uur te melden is het handig om in de (sub)bewerkersovereenkomst een termijn op te nemen die degene die de melding zal doen in staat stelt om tijdig te melden.

Melden bij betrokkenen
Een datalek waarbij waarschijnlijk sprake is van ongunstige gevolgen voor de persoonlijke levenssfeer van betrokkenen (bijvoorbeeld het lekken van financiële gegevens) moet ook bij de betrokkenen worden gemeld. U hoeft de betrokkenen niet in te lichten als de gegevens voldoende sterk versleuteld zijn en u nog een kopie hebt van de verloren gegevens. Wanneer u twijfelt, kunt u met de Autoriteit Persoonsgegevens overleggen of melding bij betrokkenen nodig is.
Het foutief adresseren van een enveloppe met de aangiften inkomstenbelasting van een echtpaar, zal bij hen gemeld moeten worden.
Het kwijtraken van een usb-stick met persoonsgegevens, die met behulp van goede encryptie is versleuteld zal vermoedelijk niet bij betrokkenen gemeld moeten worden (mits er een back up van de gegevens voorhanden is)

Wat als ik niet meld?
Wanneer u zich niet houdt aan de Wet Bescherming Persoonsgegevens (waarvan melden datalekken een onderdeel is) loopt u het risico dat de Autoriteit Persoonsgegevens u als overtreder een boete oplegt die kan oplopen tot € 820.000 of - indien dat passender is - 10% van de (wereldwijde) jaaromzet.

Wat betekent?

- *Persoonsgegevens*
  Gegevens die een natuurlijk persoon direct of indirect kunnen identificeren.
  Naam, BSN en (herkenbare) afbeeldingen zijn bijvoorbeeld persoonsgegevens.
  Adressen van BV's zijn geen persoonsgegevens

- *Verwerking van persoonsgegevens*
  Alle denkbare handelingen met betrekking tot persoonsgegevens. De Wet bescherming persoonsgegevens bevat een zeer ruime definitie van verwerken.
  Het aanmaken van een adressenbestand is verwerken, maar ook het aansluiten van een verzamelloonstaat met namen en BSN nummers aan het grootboek en het wissen van oude klantgegevens.

- *Datalekken*
  Toegang tot, vernietiging van, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Het gaat dus niet alleen om het vrijkomen van gegevens, maar ook om de onrechtmatige verwerking van gegevens. Er moet sprake zijn van een inbreuk op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden[1].
  Het kwijtraken van een usb stick met IB bestanden of de ontdekking van malware op uw server kan een datalek zijn wanneer er (persoons)gegevens verloren zijn gegaan of wanneer u niet kunt uitsluiten dat onbevoegden kennis hebben kunnen nemen van de inhoud de van de (persoons)gegevens. Ook het plaatsen van gegevens op de intranetsite van een bedrijf of instelling kan hieronder vallen.

- *Verantwoordelijke*
  Degene die het doel vaststelt van de verwerking van (persoons)gegevens en op welke wijze dat gebeurt.
  De ondernemer is "verantwoordelijke" als het gaat om de loongegevens van zijn werknemers maar ook voor klantenbestanden waarin namen van contactpersonen zijn opgenomen of gegevens van privé personen.
  De accountant is meestal verantwoordelijke wanneer hij een jaarrekening controleert of samenstelt. Ook bij de aangifte inkomstenbelasting kan de accountant als (functionele) verantwoordelijke worden gezien. En natuurlijk is de accountant verantwoordelijk als het gaat om zijn eigen bestand met klanten/ natuurlijke personen of de loonadministratie van zijn

1 Overgenomen van de Autoriteit Persoonsgegevens. Zie: https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

kantoor.

- *Bewerker*
  Degene die in opdracht (niet in loondienst) van een verantwoordelijke op zijn aanwijzingen persoonsgegevens verwerkt. *De accountant die de loonadministratie voor een ondernemer verzorgt is een bewerker. Dit speelt ook wanneer hij een opstelling maakt van persoonsgegevens in opdracht van anderen (pensioengegevens).*

- *Subbewerker*
  De subbewerker[2] verwerkt de gegevens in de regel in opdracht van de bewerker.
  Wanneer een accountant de loonadministratie doormiddel van een SaaS oplossing bijhoudt is de SaaS-leverancier een subbewerker. En als de servers van een accountant bij een host staan, is de hostingleverancier een subbewerker.

Waar vind ik meer informatie?

In deze brochure zijn alleen de meest relevante datalek-onderwerpen voor de MKB praktijk behandeld. Er zijn echter nog diverse aandachtspunten die relevant kunnen zijn. De regelgeving over datalekken is pas op 1 januari 2016 ingevoerd. Er is daarom nog veel ruimte voor verschillende interpretaties. Ook is er nog weinig jurisprudentie, zodat grensgevallen van wel of niet melden onduidelijk kunnen zijn.

Advies

Wij adviseren u om steeds actuele informatie te raadplegen.

Bijvoorbeeld;

- De Wet Bescherming Persoonsgegevens; http://wetten.overheid.nl/BWBR0011468/2016-01-01
- De informatie en de beleidsregels van de Autoriteit Persoonsgegevens op het gebied van datalekken; https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken
- De informatie en de model bewerkersovereenkomsten op de NBA site: https://www.nba.nl/Voor-leden/Diensten/Modellen-bewerkersovereenkomst/

2 'Subbewerker' is geen begrip dat in de wet is opgenomen of gedefinieerd.

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

NBA

Antonio Vivaldistraat 2 - 8
1083 HP Amsterdam
Postbus 7984
1008 AD Amsterdam

T 020 301 03 01
E nba@nba.nl
I www.nba.nl