Procedure meldplicht datalekken

Beheerder	Rien Romijn

Binnen Romijn & Lenders Assurantiën worden de persoonsgegevens van klanten en de medewerker zorgvuldig verwerkt. Mocht desondanks toch een datalek ontstaan dan zal conform onderstaande procedure worden gehandeld.

1. Bij een datalek is er sprake van een inbreuk op de beveiliging van persoonsgegevens. De persoonsgegevens zijn dan blootgesteld aan verlies of onrechtmatige verwerking.

2. Binnen ons kantoor kunnen onder andere op onderstaande wijze datalekken ontstaan:
   a. Moedwillig handelen; cybercriminaliteit, hacking, identiteitsfraude, malwarebesmetting.
   b. Technisch falen; ICT-storingen.
   c. Menselijk falen; te eenvoudige wachtwoorden, het verstrekken van username/ wachtwoord aan collega's of externen, verzenden van email met emailadressen van alle geadresseerden, email naar verkeerde ontvanger.
   d. Calamiteiten; brand op ons kantoor of extern datacentrum, wateroverlast, blikseminslag.
   e. Verlies of diefstal; USB-stick, laptop, smartphone, tablet, harde schijf.
   f. Onbereikbaarheid persoonsgegevens; niet beschikbaar zijn van digitaal polisdossier.
   g. Bovenstaande opsomming is niet limitatief, neem bij twijfel contact op met de directie of een bepaald voorval als datalek is aan te merken.

3. Indien het datalek zou kunnen leiden tot een aansprakelijkheidsstelling dan wordt terstond de verzekeraar geïnformeerd. Alle verdere stappen in de communicatie over het datalek naar betrokkenen vinden vervolgens plaats na overleg met de verzekeraar. Tevens wordt de verzekeraar ingelicht in verband met eventuele dekking op de polis van overige gevolgschade.

4. De interne meldplicht binnen ons kantoor verloopt als volgt:
   a. Een hierboven genoemd datalek moet na constatering door de medewerker terstond worden gemeld bij de directie.
   b. Indien een derde zich bij ons kantoor meldt met de mededeling dat er een datalek is, wordt deze direct in contact gebracht met de directie.
   c. Indien zich een datalek voordoet bij een bewerker is deze verplicht om zo spoedig mogelijk, doch uiterlijk binnen 48 uur na constatering, hiervan melding te maken bij de directie van ons kantoor.
   d. Datalekken worden behandeld door de directie.
   e. In eerste instantie wordt door ons kantoor, eventueel in overleg met derden, op basis van bijgevoegd schema beoordeeld of er redelijkerwijs kan worden aangenomen dat de inbreuk leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking, waaraan nadelige gevolgen voor de privacy van de betrokkenen zijn verbonden.
      i. Is dit niet het geval dan vindt alleen een interne registratie plaats van de melding
      ii. Is dit wel het geval dan meldt de directie het datalek bij de Autoriteit Persoonsgegevens
   f. De directie bepaalt de noodzakelijke vervolgacties met betrekking tot het datalek, zijnde:
      i. Lek onmiddellijk dichten
      ii. Toegang tot informatie beperken
      iii. Meer informatie vergaren over de indringer

g. De directie beoordeelt of er sprake is van eigen aansprakelijkheid of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsverplichting is geschonden of in strijd met een contractuele verplichting onvoldoende beveiliging is gerealiseerd) of onrechtmatige daad.
h. De directie stelt vast of er sprake is van strafrechtelijke verwijtbaarheid en/of al dan niet aangifte gedaan moet worden. Dit kan bijvoorbeeld spelen wanneer er sprake is van betrokkenheid vanuit ons kantoor zelf, een bewerker, of wanneer er onvoldoende maatregelen zijn getroffen om ongeregeldheden te voorkomen.
i. De directie communiceert naar de overige medewerkers binnen ons kantoor over het datalek en hoe te handelen.
j. De directie bepaalt wat er extern gecommuniceerd wordt en op welk moment. Door de directie wordt vastgesteld of de pers geïnformeerd moet worden.
k. De directie bepaalt of betrokkenen, andere partijen en/of AFM geïnformeerd moeten worden.

5. Indien voor een correcte melding van het datalek naast de beschikbare gegevens aanvullende informatie nodig is, wordt deze opgevraagd bij betreffende derde partijen als systeembeheerder, datacenter, e.d..

6. Alle datalekken worden door de directie direct na constatering digitaal geregistreerd en vastgelegd in de map Registratie datalekken.

7. Van een datalek worden minimaal de volgende gegevens in de registratie opgenomen:
   a. Datum en tijd van het datalek
   b. Naam van de melder
   c. Aard van de inbreuk (is er een aanmerkelijk risico op verlies of onrechtmatige verwerking?)
   d. Welke persoonsgegevens het betreft
   e. Het aantal records/gegevens waar het om gaat
   f. Welke groepen personen betrokken zijn bij het datalek
   g. Welke (verbeter)maatregelen er door ons kantoor cq. bewerker zijn of worden genomen
   h. Contactpersoon voor deze melding

8. Indien het datalek veroorzaakt is door één of meerdere personeelsleden die onder verantwoordelijkheid van ons kantoor werken, informeert de directie de betrokkene(n) over het datalek en vraagt hen om commentaar. Hiervan wordt een schriftelijke samenvatting gemaakt en na ondertekening door betrokkene(n) aan het personeelsdossier toegevoegd.

Melding Autoriteit Persoonsgegevens

9. Als de directie over alle informatie beschikt, zet deze de melding door naar de Autoriteit Persoonsgegevens. Dit gebeurt uiterlijk binnen 72 uur na constatering van het datalek. In deze melding is minimaal opgenomen:
   a. Aard van de inbreuk, waaronder betrokken categorieën, aantal betrokkenen, aantal gegevens.
   b. Beschrijving van de te verwachten gevolgen voor de betrokkenen volgens ons kantoor cq. de bewerker.
   c. Getroffen en/of te treffen maatregelen om de schade voor betrokkenen te verkleinen.
   d. Maatregelen die betrokkenen kunnen nemen om verdere schade te verkleinen, inclusief de wijze van inlichten hierover.
   e. Contactpersoon binnen ons kantoor voor betrokkenen.

10. Indien de informatie voor de melding nog niet compleet is, worden binnen de wettelijke termijn van 72 uur beschikbare gegevens gemeld en wordt de melding later aangevuld.

11. Bij twijfel wel of niet melden worden binnen de wettelijke termijn van 72 uur beschikbare gegevens gemeld en kan de melding op een later tijdstip eventueel alsnog worden ingetrokken.

12. De ontvangstbevestiging van de Autoriteit Persoonsgegevens zal worden toegevoegd aan het dossier.

13. Indien de Autoriteit Persoonsgegevens nadere informatie wenst omtrent de melding van het datalek, zal deze direct in contact worden gebracht met de directie van ons kantoor. Zonder toestemming van de directie zal door de medewerker van ons kantoor geen uitspraken over de melding worden gedaan aan de Autoriteit Persoonsgegevens.

Melding Autoriteit Financiële Markten

14. Indien melding wordt gemaakt van het datalek bij de Autoriteit Persoonsgegevens, is ons kantoor in het kader van de Wft verplicht om van het datalek ook een incidentenmelding te maken. Zie hiervoor de procedure '*Behandeling incidenten en -registratie'*.

Berichtgeving aan betrokkenen

15. Na melding bij de Autoriteit Persoonsgegevens worden de betrokkenen schriftelijk op de hoogte gesteld. Deze brief of email bevat in ieder geval onderstaande informatie:
    a. Aard van de inbreuk
    b. Aard van de informatie die is 'gelekt'
    c. Te ondernemen actie door betrokkene(n) om verdere schade te verkleinen
    d. De contactpersoon binnen ons kantoor die voor vragen over het datalek door de betrokkenen benaderd kan worden

16. Berichtgeving aan betrokkenen kan achterwege blijven indien:
    a. De persoonsgegevens versleuteld zijn of direct na constatering op afstand gewist zijn.
    b. Indien er zwaarwegende bedrijfsbelangen zijn om betrokkenen niet in kennis te stellen. De Autoriteit Persoonsgegevens kan te allen tijde verlangen dat betrokkenen alsnog worden geïnformeerd.

Bijlage:
Modelbrief betrokkene(n) meldplicht datalekken
Registratieformulier meldplicht datalekken