Protocol datalekken – Kuiken Accountancy BV

Gebruikte afkortingen:

KA	Kuiken Accountancy BV
FG	Functionaris Gegevesbescherming; Kuiken Accountancy BV heeft Maarten Evers aangesteld als FG
WBP	Wet bescherming persoonsgegevens
AP	Autoriteit Persoonsgegevens

1. Inleiding

1.1. Dit document beschrijft de handelingen te verrichten door KA bij een datalek zoals gedefinieerd in de WBP.

1.2. Van een datalek is sprake bij een inbreuk op de beveiliging van persoonsgegevens (als bedoeld in artikel 13 van de Wbp). De persoonsgegevens zijn dan blootgesteld aan verlies of onrechtmatige verwerking.

1.3. Een datalek dient onverwijld te worden gemeld aan de AP, en in bepaalde gevallen ook aan de betrokkene(n). De betrokkene is degene van wie persoonsgegevens zijn gelekt.

1.4. De meldplicht is eveneens van toepassing op KA als het datalek bij een derde is ontstaan, bijvoorbeeld een bewerker van persoonsgegevens van KA (‘Bewerker’).

2. Identificatie van een datalek: organisatie

2.1. De medewerker die een (mogelijk) datalek constateert, meldt dit incident per omgaande bij de FG van KA.

2.2. Een medewerker van KA of een Bewerker is te allen tijde bevoegd zelfstandig een melding te doen aan de FG. De procedure meldplicht datalekken als omschreven in dit protocol wordt dan gestart.

3. Wanneer moet een datalek worden gemeld?

Niet alle incidenten hoeven aan de AP te worden gemeld. Alleen incidenten die voldoen aan de volgende criteria moeten worden gemeld:

- een incident waarvoor een ‘aanzienlijke kans’ bestaat op ernstige nadelige gevolgen voor de personen van wie de gegevens zijn zoekgeraakt;
- een incident die ernstige gevolgen kan hebben voor de bescherming van persoonsgegevens (bijvoorbeeld het verliezen van een gegevensdrager met persoonsgegevens) .

Of een datalek aan de AP en/of betrokke(n) moet worden gemeld is afhankelijk van de volgende afwegingen.

4. Identificatie van een incident/is er sprake van een datalek?

4.1. De FG draagt zo spoedig mogelijk zorg voor het inventariseren en verzamelen van de informatie die benodigd is voor identificeren van het (eventuele) datalek. Daarbij kan het formulier van de AP voor het melden van datalekken als uitgangspunt dienen. Het formulier is te vinden op het volgende adres: https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken

4.2. Wanneer op basis van de verzamelde informatie het vermoeden van een datalek bestaat wordt in overleg tussen de FG en de eventuele overige verantwoordelijke en/of betrokken personen in de organisatie van KA of de betreffende Bewerker, beoordeeld of daadwerkelijk sprake is van een datalek.

4.3. In dat overleg kan tevens worden beoordeeld of er acuut maatregelen dienen te worden genomen om de schade zoveel mogelijk te beperken, waaronder het doen van een (voorlopige) melding aan betrokkenen. Indien nodig kan advies gevraagd worden aan een juridisch adviseur en/of een communicatieadviseur.

4.4. Wanneer er sprake is van een incident dat gemeld moet worden aan de AP kan gebruik worden gemaakt van de overzichten in de beleidsregels 'Meldplicht datalekken in de Wet bescherming persoonsgegevens' van de AP welke zijn te vinden op het volgende adres:

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf

4.5. Bij de beoordeling van de vraag of sprake is van een datalek zijn de volgende factoren van belang:

- is er sprake van onrechtmatige verwerking van persoonsgegevens?
  Hiermee wordt onder andere gedoeld op de onbedoelde of onwettige vernietiging, verlies of wijziging van verwerkte persoonsgegevens of een niet toegestane toegang tot verwerkte persoonsgegevens of de niet toegestane verstrekking daarvan;
- is er sprake van verlies van persoonsgegevens?
  Dit betekent dat KA (of feitelijk haar Bewerker) deze gegevens niet meer heeft, omdat ze zijn vernietigd of op een andere wijze verloren zijn gegaan;
- is er sprake van een enkele tekortkoming of kwetsbaarheid in de beveiliging?
  Kan er redelijkerwijs worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid?
- zijn er persoonsgegevens van gevoelige aard gelekt?
  Bijzondere persoonsgegevens (artikel 16 Wbp) zijn onder andere
    - gegevens over de financiële of economische situatie van de betrokkene;
    - gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
    - gebruikersnamen, wachtwoorden en andere inloggegevens; en
    - gegevens die kunnen worden gebruikt voor (identiteits)fraude;
- leiden de aard en de omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?
  Bij de beoordeling of daarvan sprake is zijn onder andere van belang:
    - de omvang van de verwerking;
    - de vraag of het om veel persoonsgegevens per persoon gaat en/of om gegevens van grote groepen betrokkenen;
    - de impact van het verlies of de onrechtmatige verwerking van persoonsgegevens;
    - het delen van de persoonsgegevens met derden waardoor de gevolgen van verlies en onbevoegde wijziging van persoonsgegevens ook elders impact kunnen hebben; en
    - betrokkenheid van kwetsbare groepen.

4.6. Indien het incident niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens is er geen sprake van een datalek maar van een beveiligingslek. In dat geval is melding aan de AP niet nodig.

4.7. Indien tot de conclusie wordt gekomen dat sprake is van een (mogelijk) datalek, wordt het communicatietraject richting betrokkene(n) en (eventueel) de betreffende Bewerker tussen de directie van KA en de FG besproken.

5. Melden aan de Autoriteit Persoonsgegevens

5.1. De FG verzorgt de tijdige melding bij de AP volgens het hierboven onder 4.1 genoemde meldingsformulier van de AP. De melding dient op grond van de Wbp onverwijld, zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek te geschieden.

5.2. De FG fungeert als contactpersoon inzake de communicatie met de AP. Afhankelijk van de aard van het datalek of indien blijkt dat het incident geen datalek is kan de melding aan de AP worden aangevuld of ingetrokken.

5.3. De FG draagt ervoor zorg dat de bij het incident betrokken medewerkers worden geïnformeerd en vraagt de bij het incident betrokken medewerkers zo snel mogelijk een verslag op te stellen over de toedracht van het incident. Deze schriftelijke informatie wordt aan de FG verstrekt ten behoeve van het datalekkendossier van KA.

5.4. Na ontvangst van de melding aan de AP zal de AP daarvan een ontvangstbevestiging sturen. De AP neemt alleen contact op indien de AP daartoe aanleiding ziet.

6. Dient het datalek te worden gemeld aan betrokkene(n)?

6.1. Indien een datalek is gemeld aan de AP dient te worden vastgesteld of het datalek ook moeten worden gemeld aan degenen om wiens persoonsgegevens het gaat. De FG zal dat vaststellen.

6.2. De beoordeling of er sprake is van een incident dat gemeld moet worden aan de betrokkenen kan tot stand komen met behulp van de overzichten in de beleidsregels ‘Meldplicht datalekken in de Wet bescherming persoonsgegevens’ van de AP zoals hiervoor genoemd.

6.3. Bij de afweging of het datalek dient te worden gemeld aan betrokken is onder andere het volgende van belang:

- indien KA passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor een ieder die geen recht heeft op kennisname van de gegevens, dan kan de melding aan de betrokkene(n) achterwege blijven. Indien daarover wordt getwijfeld dan dient het datalek aan de betrokkene(n) gemeld te worden;
- het datalek moet aan de betrokkene(n) worden gemeld indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer;
- Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. De schade kan van materiële of van immateriële aard zijn, waarbij kan worden gedacht aan onrechtmatige publicatie, aantasting in eer en goede naam, identiteitsfraude of discriminatie;

6.4. De melding aan de betrokkene(n) mag achterwege blijven als daarvoor zwaarwegende redenen aanwezig zijn. De melding mag alleen achterwege mag blijven als dit noodzakelijk is met het oog op de belangen die

worden genoemd in artikel 43 Wbp ((i) de veiligheid van de staat, (ii) de voorkoming, opsporing en vervolging van strafbare feiten, (iii) gewichtige economische en financiële belangen van de staat en andere openbare lichamen, (iv) het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen, bedoeld onder (ii) en (iii), of (v) de bescherming van de betrokkene of van de rechten en vrijheden van anderen).

7. Handelwijze melding aan betrokkene(n)

7.1. De FG stelt in samenspraak met de communicatieadviseur en juridisch adviseur een kennisgeving aan betrokkene(n) op. De FG bepaalt wat aan de betrokkene(n) wordt gemeld.

7.2. De melding bevat in ieder geval de aard van de inbreuk, contactgegevens van KA en een contactpersoon of informatiepunt waar de betrokkene(n) meer informatie over de inbreuk kan (kunnen) krijgen en de maatregelen die KA de betrokkene(n) aanbeveelt om te nemen om de negatieve gevolgen van de inbreuk te beperken.

7.3. Het datalek moet onverwijld gemeld worden aan de betrokkene(n). Dit betekent dat KA na het ontdekken van het datalek enige tijd mag nemen voor nader onderzoek zodat KA de betrokkene op een behoorlijke en zorgvuldige manier kan informeren. Daarbij dient te allen tijde rekening te worden gehouden met het (eventuele) feit dat de betrokkene(n) naar aanleiding van de melding mogelijk maatregelen moet(en) nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder de betrokkene(n) daarover wordt geïnformeerd, hoe eerder deze in actie kan komen.

7.4. De betrokkene(n) worden individueel geïnformeerd.

7.5. In de melding aan de AP is aangegeven of het datalek aan betrokkene(n) is gemeld. Indien de aan de AP aangegeven termijn waarbinnen die melding zou worden gedaan aan de betrokkene(n) niet kan worden gehaald dan dient de FG dit aan de AP door te geven door middel van een aanpassing van de eerdere melding.

8. Datalek-onderzoek en vaststellen verbetermaatregelen

8.1. De FG stelt zo spoedig mogelijk na de vaststelling van het incident een (intern) onderzoek in naar de feitelijke toedracht van het (mogelijke) datalek en betrekt daarbij de vraag of en hoe dergelijke incidenten in de toekomst kunnen worden voorkomen.

8.2. De FG mag daartoe met medewerkers van KA en/of overige relevante personen (zoals eventueel medewerkers van de Bewerker(s) van KA) spreken, alle relevante documenten inzien en toegang hebben tot alle plaatsen, voor zover noodzakelijk voor een zorgvuldig onderzoek;

8.3. De FG kan voorstellen om waar nodig externe partijen te betrekken indien dat voor een deugdelijk onderzoek noodzakelijk is.

8.4. De FG rapporteert de conclusies van het hiervoor bedoelde onderzoek zo spoedig mogelijk.

8.5. In overleg waarbij in ieder geval de FG aanwezig is zullen de uitkomsten van het hiervoor genoemde onderzoek worden besproken en afspraken worden gemaakt over verbetermaatregelen om herhaling van het incident zoveel mogelijk te voorkomen.

8.6. De directie van KA stelt vast welke verbetermaatregelen worden geïmplementeerd en ziet er op toe dat de vastgestelde verbetermaatregelen worden geïmplementeerd en in de organisatie van KA (en waar nodig extern, zoals aan een Bewerker) worden gecommuniceerd.

9. Datalek-dossier

Het datalek-dossier wordt digitaal bij de FG bewaard voor de duur van minimaal 1 jaar. Er kan een langere termijn van minimaal 3 jaar van toepassing zijn zoals bedoeld in de beleidsregels ‘Meldplicht datalekken in de Wet bescherming persoonsgegevens’ van de AP, pagina 46.