METROPOOL REGIO EINDHOVEN

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 1118

2 augustus 2018

Officiële uitgave van de gemeenschappelijke regeling Metropoolregio Eindhoven

Datalekkenprotocol Metropoolregio Eindhoven

HOOFDSTUK 1 ALGEMEEN

Sinds 1 januari 2016 geldt in Nederland de meldplicht datalekken. Kort gezegd houdt de meldplicht in dat bedrijven, overheden en andere organisatie onverwijld een melding moeten doen bij de Autoriteit Persoonsgegevens (hierna: "AP") indien sprake is van een ernstig datalek.

Een datalek dient binnen 72 uur nadat een organisatie van het datalek op de hoogte is gebracht of geraakt te worden gemeld aan de AP. In sommige gevallen dient het datalek ook bij de betrokkenen (de mensen van wie persoonsgegevens zijn gelekt) gemeld te worden. Daarnaast is het in een aantal gevallen raadzaam om derden op de hoogte te stellen van het datalek.

Datalekken kunnen binnen iedere organisatie plaatsvinden. Voorbeelden hiervan zijn verlies of diefstal van een USB-stick, laptop, tablet of smartphone, inbreuk door een hacker en calamiteiten door bijvoorbeeld brand of een overstroming.

Een datalek kan grote gevolgen hebben voor de betrokkenen van wie de gegevens zijn gelekt. Te denken valt aan schade als gevolg van identiteitsfraude, discriminatie of reputatieschade. Ook voor de organisatie kan een datalek grote gevolgen hebben, waarbij gedacht kan worden aan reputatieschade, verlies van klanten en (hoge) boetes die door de AP kunnen worden opgelegd.

In dit protocol wordt uiteengezet wanneer sprake is van een datalek, hoe datalekken gesignaleerd kunnen worden en wanneer het datalek gemeld moet worden aan de AP en aan betrokkenen.

HOOFDSTUK 2 BEGRIPPEN

In dit hoofdstuk wordt kort ingegaan op de belangrijkste begrippen rondom een datalek.

2.1 Persoonsgegevens

Een datalek wordt omschreven als "iedere situatie waarin persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking" . Om te kunnen beoordelen of sprake is van een datalek dient allereerst duidelijk te zijn wat het begrip "persoonsgegevens" inhoudt.

Een persoonsgegeven is "elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon". Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld. Voorbeelden van persoonsgegevens zijn gegevens zoals naam, adres en woonplaats. Daarnaast kunnen ook documenten/bestanden als e-mails, medische dossiers, foto's en camerabeelden persoonsgegevens bevatten.

Naast bovenstaande voorbeelden van persoonsgegevens kent de wet ook bijzondere categorieën van persoonsgegevens, de zogenoemde gevoelige persoonsgegevens (art. 16 Wbp) . Onder gevoelige persoonsgegevens worden gegevens verstaan over iemands:

- Godsdienst of levensovertuiging;

- Ras;

- Politieke gezindheid;

- Gezondheid;

- Seksuele leven;

- Lidmaatschap van een vakvereniging;

- Strafrechtelijke persoonsgegevens;

- Onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

Het Burgerservicenummer en overige identificatienummers kwalificeren tevens als bijzondere persoonsgegevens.

Ook op het moment dat er geen sprake is van een lek met betrekking tot bovenstaande gevoelige persoonsgegevens kan er toch sprake zijn van een datalek. Dit is afhankelijk van de aard en omvang van de inbreuk.

2.2 Verwerking van persoonsgegevens

Onder verwerking van persoonsgegevens als bedoeld in art. 1 sub b Wbp wordt verstaan: “elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.”

Van verwerking van persoonsgegevens is sprake wanneer door Metropoolregio Eindhoven bijvoorbeeld klantgegevens of personeelsgegevens worden verwerkt.

2.3 Verantwoordelijke (verwerkingsverantwoordelijke) en bewerker (verwerker)

Krachtens art. 1 sub d Wbp is de verantwoordelijke de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

De bewerker in de zin van art. 1 sub e Wbp is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

2.4 Bewerkersovereenkomst

Op het moment dat een partij de verwerking van persoonsgegevens uitbesteedt aan een andere partij is het wettelijk verplicht om afspraken vast te leggen in een bewerkersovereenkomst. In deze overeenkomst worden onder meer afspraken met betrekking tot de doeleinden voor de verwerking, de beveiligingsmaatregelen en de toezicht door de verantwoordelijke vastgelegd.

Metropoolregio Eindhoven heeft voor diverse gegevensverwerkingen derden ingeschakeld als bewerker. Metropoolregio Eindhoven heeft met al deze bewerkers een bewerkersovereenkomst gesloten. Bij toekomstige inschakeling van derden als bewerker zal Metropoolregio Eindhoven de standaard bewerkersovereenkomst gebruiken. Het overzicht van de bewerkers wordt voortdurend geactualiseerd en is bijgesloten als bijlage 1.

2.5 Datalek

Een datalek kan opzettelijk of onopzettelijk zijn veroorzaakt. Een voorbeeld van een opzettelijke datalek is het verwerven van vertrouwelijke informatie via e-mail of internet (phishing). Een voorbeeld van een onopzettelijke datalek is het verlies van een niet-beveiligde gegevensdrager, zoals een USB-stick.

Een datalek dient aan de AP te worden gemeld als het lek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens (artikel 34a, lid 1, Wbp). Het datalek moet daarnaast ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (artikel 34a, lid 2, Wbp).

Bij het beoordelen van (de impact van) het datalek dient allereerst te worden onderzocht waar het datalek heeft plaatsgevonden en wat de oorzaak is. Dit is van belang om te beoordelen of het datalek al voorbij is of dat het nog door loopt (en of de aanvaller nog actief is). Vervolgens dient bekeken te worden hoe het lek gestopt kan worden. Er dient tevens te worden beoordeeld wat voor (persoons)ge-

gevens en van hoeveel personen er gegevens gelekt zijn, hoe groot de nadelige gevolgen voor de betrokkenen zouden kunnen zijn en hoe groot het risico is dat de nadelige gevolgen ook daadwerkelijk zullen optreden.

Voor de beoordeling van het datalek worden speciale teams ingezet, waarover meer in het volgende hoofdstuk.

2.6 De Autoriteit Persoonsgegevens (AP)

De Autoriteit Persoonsgegevens (AP) is de toezichthoudende autoriteit die toezicht houdt op de naleving van de wettelijke regels voor de bescherming van persoonsgegevens. Indien Metropoolregio Eindhoven in strijd met de meldplicht datalekken handelt, is de AP (op grond van art. 66 Wbp) bevoegd om een bestuurlijke boete op te leggen.

HOOFSTUK 3 ROLLEN EN TEAMS

Na de ontdekking van een datalek dienen de volgende teams en personen te worden opgeroepen:

- Het datalekteam;

- Het ICT-responseteam;

- De proceseigenaar.

3.1 Het datalekteam

Het datalekteam bestaat uit een data protection officer/functionaris voor de gegevensbescherming, information security officer (ISO), de proceseigena(a)ren en in de meeste gevallen iemand van de directie. Het datalekteam onderzoekt en beoordeelt het datalek vanuit privacy-oogpunt en bepaalt hoe gehandeld moet worden. Het team onderzoekt o.a.:

- Wat voor persoonsgegevens er bij het datalek betrokken zijn;

- Wat er met de gegevens is gebeurd;

- Of de gegevens daadwerkelijk gelekt zijn;

- Hoe groot de impact van het datalek is (voor zowel de betrokkenen als de organisatie).

Het datalekteam van Metropoolregio Eindhoven bestaat uit de volgende leden:

- Functionaris voor de gegevensbescherming;

- Directeur Metropoolregio Eindhoven

- ICT Service Manager Metropoolregio Eindhoven

Het datalekteam houdt een incidentenregistratie bij waarin zij (vermoedens van) datalekken rapporteert. Het datalekteam beoordeelt of het datalek bij de AP gemeld dient te worden. Bij twijfel of het datalek moet worden gemeld, wordt geadviseerd om het datalek (uit voorzorg) bij de AP te melden.

3.2 Het ICT-responseteam

Het ICT-responseteam bestaat meestal uit netwerk- en systeembeheerders. Dit team richt zich op het onderzoek naar en de bestrijding van het datalek. Het ICT-responseteam kan er voor zorgen dat systemen worden uitgeschakeld, apparatuur wordt losgekoppeld van het computernetwerk en dat bepaalde gebruikersaccounts worden geblokkeerd.

Daarnaast richt het ICT-responseteam zich op het herstellen van processen op ICT-gebied binnen de organisatie.

Het ICT-responseteam van Metropoolregio Eindhoven bestaat uit de volgende leden:

- ICT Service Manager Metropoolregio Eindhoven;

- ICT Service Manager van de ICT Dienstverlener;

- Senior netwerk beheerder van de ICT Dienstverlener;

- Senior systeem beheerder van de ICT Dienstverlener;

De ICT-afdeling dient in opdracht van het ICT-responseteam back-ups en kopieën van systemen en bestanden te maken.

3.3 De proceseigenaar

De proceseigenaar is degene die binnen een proces de leiding heeft en die het proces aanstuurt. Het is van belang om de proceseigenaar bij het datalek te betrekken, zodat duidelijk gerapporteerd kan worden wat voor impact het datalek op de processen van Metropoolregio Eindhoven heeft.

HOOFDSTUK 4 MELDINGSPROTOCOL

Stap 1 Vermoeden van beveiligingsincident/datalek

Op het moment dat iemand binnen Metropoolregio Eindhoven het vermoeden heeft dat zich een beveiligingsincident/datalek heeft voorgedaan, dient dit onmiddellijk te worden gemeld aan het datalekteam. Het datalekteam is te bereiken op telefoonnummer 040-2594594 en op e-mailadres fg@metropoolregioeindhoven.nl.

Stap 2 Verzamelen van informatie

Het is van belang om zoveel mogelijk informatie over het beveiligingsincident/datalek te verzamelen en vast te leggen. Hier bij kan onder meer gedacht worden aan:

- Een omschrijving van het incident.

- Een schatting van het aantal personen waarvan de gegevens zijn gelekt.

- De categorie personen waarvan de gegevens zijn betrokken.

- Het soort persoonsgegevens.

- Gegevens wanneer de inbreuk op de beveiliging plaatsvond.

- De aard van de inbreuk.

- De gevolgen van de inbreuk.

- De ondernomen acties.

Ter beoordeling van het incident kan Metropoolregio Eindhoven de volgende vragen stellen:

1. Waar heeft het incident plaatsgevonden?

a. Op de infrastructuur van de eigen organisatie.

b. Op de infrastructuur buiten de eigen organisatie.

2. Welke systemen zijn betrokken?

3. Waar heeft het verlies/de diefstal van fysieke gegevensdragers (laptop, tablet, smartphone, USB-stick, dossier) plaatsgevonden en onder welke omstandigheden?

4. Om wat voor data gaat het?

a. Persoonsgegevens;

i. Wat voor persoonsgegevens.

ii. Van hoeveel personen?

b. Overige informatie.

5. Waar heeft het incident invloed op?

a. De vertrouwelijkheid van de gegevens (bijvoorbeeld wanneer deze gelezen worden door een onbevoegde persoon).

b. De betrouwbaarheid/integriteit van de gegevens (bijvoorbeeld wanneer deze onbedoeld zijn gewijzigd).

c. De beschikbaarheid van de gegevens (bijvoorbeeld wanneer deze zijn verloren of verwijderd).

6. Welke bedrijfsprocessen hebben het grootste probleem?

7. Wat is de oorzaak?

a. Verkeerde gegevensverstrekking.

b. Verlies van gegevensdragers.

c. Misbruik van autorisatie.

d. Kwaadwillende oorzaak van buiten de organisatie.

e. Kwaadwillende oorzaak vanuit eigen organisatie.

f. Systeemfout of andere technische fout of overmacht.

8. Is het datalek voorbij of duurt het nog steeds voort?

De verzamelde gegevens worden opgeslagen in Afas, conform de procesbeschrijving “Melding datalek”. De informatie wordt bewaard voor een termijn van drie jaar na ontdekking van het datalek.

Stap 3 Te ondernemen acties

Nadat is vastgesteld dat sprake is van een datalek zijn er drie zaken die onmiddellijke aandacht vragen:

- De bestrijding van het datalek door het ICT-responseteam.

- De melding van het datalek bij de AP.

- De melding van het datalek aan de betrokkenen.

Melden datalek AP

Of een datalek bij de AP gemeld dient te worden, is afhankelijk van een aantal factoren. In een aantal situaties is de meldplicht niet van toepassing. Dit is het geval bij:

- Gegevensverzamelingen “op papier” die niet bestemd zijn om in een bestand te worden opgenomen.

- Gegevensverwerkingen die uitsluitend worden gebruikt voor journalistieke, artistieke en literaire doeleinden.

- Gegevensverwerking die vallen onder één van de volgende wetten:

o Kieswet.

o Wet basisregistratie personen (Wbrp).

o Wet op de inlichtingen- en veiligheidsdiensten (Wivd).

o Wet justitiële en strafvorderlijke gegevens (Wjsg).

o Wet politiegegevens (Wpg).

Om te beoordelen of het datalek bij de AP gemeld dient te worden, dienen de volgende vragen te worden beantwoord:

- Is de meldplicht datalekken uit de Wbp van toepassing?

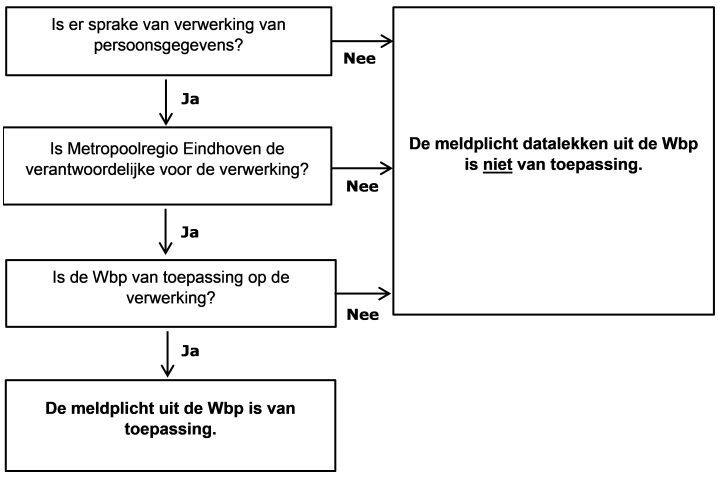
- Kan het beveiligingsincident worden gekwalificeerd als een datalek?

- Heeft het datalek (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens?

In het navolgende worden bovenstaande vragen met behulp van stroomschema’s opgesplitst in deelvragen. Voor de betekenis van de begrippen wordt verwezen naar Hoofdstuk 2 van dit Datalekkenprotocol.

Schema 1: Is de meldplicht datalekken uit de Wbp van toepassing?

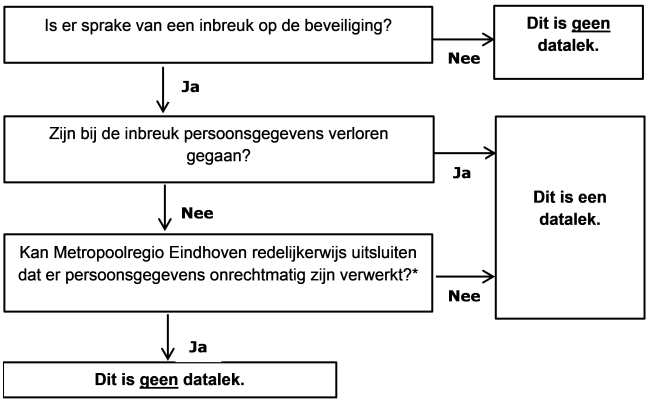
Schema 1: Is de meldplicht datalekken uit de Wbp van toepassing?



Vervolgens dient beoordeeld te worden of het beveiligingsincident gekwalificeerd kan worden als een datalek. Dit kan aan de hand van het volgende schema worden vastgesteld.

Schema 2: Kan het beveiligingsincident worden gekwalificeerd als een datalek?

Schema 2: Kan het beveiligingsincident worden gekwalificeerd als een datalek?



*Onder onrechtmatige vormen van verwerking wordt verstaan de aantasting van de persoonsgegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan. Als redelijkerwijs niet valt uit te sluiten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid, is de inbreuk een datalek.

Indien niet hoogst aannemelijk is dat er iets mis is gegaan met de gegevens, is er geen sprake van een datalek. Een voorbeeld hiervan is dat gegevens verloren zijn gegaan, maar dat deze gegevens terug gehaald kunnen worden door een volledige back-up.

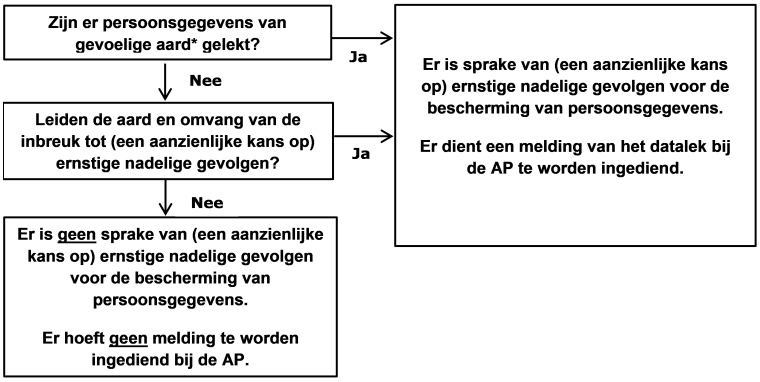
Vervolgens dient te worden beoordeeld of het datalek (een aanzienlijke kans op) ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Van “ernstige nadelige gevolgen” is sprake wanneer:

1. Persoonsgegevens van gevoelige aard zijn betrokken bij het datalek; of

2. Aanzienlijk veel persoonsgegevens zijn betrokken bij het datalek.

Schema 3: Heeft het datalek (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens?

Schema 3: Heeft het datalek (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens?



* Naast de in Hoofdstuk 2 opgesomde gevoelige persoonsgegevens, zijn de volgende gegevens volgens de AP tevens gevoelig van aard:

- iemands financiële of economische situatie (bijvoorbeeld salarisgegevens, betalingsgegevens en gegevens over schulden);

- gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene (bijvoorbeeld ingeval van een gokverslaving, prestaties op werk of school en relatieproblemen);

- gebruikersnamen, wachtwoorden en andere inloggegevens;

- gegevens die kunnen worden misbruikt voor (identiteits)fraude (bijvoorbeeld biometrische gegevens, kopieën van identiteitsbewijzen en Burgerservicenummers).

Meldingsformulier

Indien beoordeeld wordt dat het datalek dient te worden gemeld bij de AP, dient de melding binnen 72 uur na ontdekking van het lek via het digitaal loket datalekken door middel van het invullen van een online formulier op de website van de AP (www.autoriteitpersoonsgegevens.nl) door de verwerkingsverantwoordelijke te worden ingediend. De melding bevat de volgende informatie:

- De aard van de melding (nieuw of bestaand);

- Het wettelijk kader (Wbp of Telecommunicatiewet);

- Algemene informatie en contactgegevens;

- Gegevens over het datalek;

- Vervolgacties en maatregelen;

- Technische beschermingsmaatregelen;

- Internationale aspecten;

- Vervolgmelding (is de melding compleet?).

Nadat de melding is ingediend, ontvangt de melder een meldingsnummer ter bevestiging. Dit meldingsformulier dient bij verdere communicatie of bij een aanvulling op een bestaande melding te worden gebruikt.

Melden bij betrokkenen

Een datalek dient gemeld te worden aan de betrokkenen indien het datalek waarschijnlijk nadelige gevolgen heeft voor de betrokkenen. Alleen datalekken die aan de AP gemeld dienen te worden, dienen in een aantal gevallen ook aan de betrokkenen te worden gemeld. Indien dus niet aan de AP gemeld hoeft te worden, hoeft ook niet aan de betrokkenen gemeld te worden.

Er hoeft geen melding aan de betrokken te worden gedaan indien er sprake is van adequate versleuteling van de gegevens of indien de organisatie zwaarwegende belangen heeft om (nog) niet te melden. Een datalek hoeft dus niet altijd (direct) gemeld te worden bij de betrokkenen.

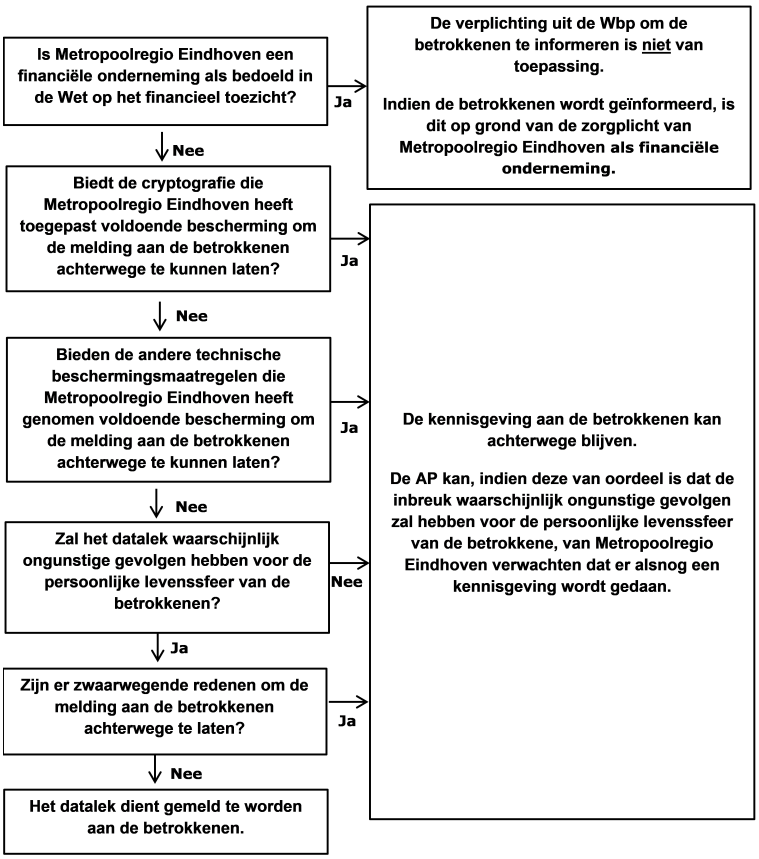
Indien een organisatie niet verplicht is om het lek aan de betrokkenen te melden, kan de organisatie er voor kiezen om dit vrijwillig te doen. Door het datalek te melden bij de betrokkenen, kunnen betrokkenen zelf maatregelen treffen om een verdere inbreuk te beperken. Betrokkenen kunnen dan bijvoorbeeld wachtwoorden wijzigen die voor meerdere accounts gebruikt worden.

Op het moment dat wordt besloten (om al dan niet vrijwillig) een melding aan de betrokkenen te doen, dient dit zo spoedig mogelijk te gebeuren. Er geldt geen specifieke termijn waarbinnen een organisatie de melding moet doen aan de betrokkenen.

Of het datalek aan de betrokkenen gemeld dient te worden, kan aan de hand van het volgende schema worden beoordeeld.

Schema 4: Dient het datalek aan de betrokkenen te worden gemeld?

Schema 4: Dient het datalek aan de betrokkenen te worden gemeld?



Uit bovenstaand schema kunnen een aantal belangrijke vragen worden afgeleid. Met betrekking tot het melden aan de betrokkenen zijn de volgende twee vragen van belang:

1. Waren de gegevens (goed) versleuteld?

o Indien ja > geen melding aan betrokkenen;

o Indien nee > ga naar de volgende vraag (2);

2. Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkenen?

o Indien ja > melden aan betrokkenen;

o Indien nee > geen melding aan betrokkenen.

De melding aan de betrokkenen betreft in ieder geval de volgende informatie:

- Wat is er aan de hand/wat zijn de gevolgen;

- Betrokkenen dienen te worden geïnformeerd waar ze terecht kunnen met vragen;

- Betrokkenen dienen te worden geïnformeerd over welke maatregelen ze eventueel zelf kunnen treffen.

Melden bij overige partijen

Naast het melden aan de AP en de eventuele melding aan de betrokkenen kan het raadzaam zijn om andere partijen op de hoogte te stellen van het datalek. Hier bij kan gedacht worden aan:

- Bestuur/Raad van commissarissen/aandeelhouders;

- Medewerkers;

- Brancheorganisaties/ketenpartners;

- Verzekering;

- Media.

Het datalekteam beslist in overleg met de proceseigenaar of het datalek aan andere partijen dient te worden gemeld. Zij stellen samen een communicatieplan op.

Voor vragen over dit protocol kan contact opgenomen worden met de Functionaris voor de Gegevensbescherming op telefoonnummer 040-2594594 of per email fg@metropoolregioeindhoven.nl.

28-05-2018

Metropoolregio Eindhoven