PROTOCOL MELDPLICHT DATALEKKEN

Per 1 januari 2016 is de meldplicht datalekken van toepassing. Deze meldplicht is geregeld in artikel 34a Wet bescherming persoonsgegevens (Wbp) en houdt in, dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben, waarbij persoonsgegevens betrokken zijn. In een aantal gevallen dient een datalek ook gemeld te worden aan de betrokkene(n).

Dit protocol beschrijft de te volgen procedure indien zich een datalek voordoet binnen Ressort Wonen of binnen de organisatie van een bewerker van Ressort Wonen, zodat een datalek adequaat wordt afgehandeld.

Artikel 1 Definities

In dit protocol verstaan wij onder:

- *Autoriteit Persoonsgegevens:* de onafhankelijke instantie, die als toezichthouder is aangesteld voor het toezicht op het verwerken van persoonsgegevens.

- *Betrokkene(n):* degene(n) van wie de persoonsgegevens zijn gelekt.

- *Bewerker:* een buiten de organisatie van Ressort Wonen staande persoon of instelling, die gegevens ten behoeve van Ressort Wonen bewerkt, dat wil zeggen overeenkomstig de instructies en onder (uitdrukkelijke) verantwoordelijkheid van Ressort Wonen.

- *Datalek:* een beveiligingsincident, waarbij sprake is van een inbreuk op de beveiliging van persoonsgegevens. Bij een dergelijk incident zijn persoonsgegevens verloren gegaan, of Ressort Wonen kan niet uitsluiten dat er persoonsgegevens onrechtmatig zijn verwerkt (aantasting van de persoonsgegevens of onbevoegde kennisneming, wijziging of verstrekking daarvan). Voorbeelden hiervan zijn:
  - een verloren/gestolen laptop, iPad, smartphone, USB-stick;
  - een hack in het ICT-systeem;
  - een malware-besmetting;
  - het slordig omgaan met het beheer van wachtwoorden, die toegang geven tot informatiebestanden;
  - het per ongeluk verkeerd adresseren van een brief of e-mail die persoonsgegevens bevat;
  - een calamiteit waarbij persoonsgegevens verloren gaan, zoals een brand in een datacentrum.

- *Ontdekker:* degene die het datalek op het spoor komt en het proces in werking moet stellen.

- *Persoonsgegevens:* alle gegevens aan de hand waarvan een natuurlijke persoon kan worden geïdentificeerd.

- *Verantwoordelijke:* degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Artikel 2 Reikwijdte

A. Dit protocol is van toepassing op situaties waarin Ressort Wonen te maken heeft met een datalek en heeft als doel het vastleggen van verantwoordelijkheden en de werkwijze bij het optreden van een datalek, zodat een datalek adequaat wordt afgehandeld.

B. De wettelijke meldplicht richt zich uitsluitend tot de verantwoordelijke. Dus ook indien zich een datalek voordoet binnen de organisatie van een bewerker van Ressort Wonen, is Ressort Wonen degene die een melding moet doen bij de Autoriteit Persoonsgegevens. Dit protocol is daarom ook van toepassing indien een bewerker aan Ressort Wonen meldt, dat de bewerker te maken heeft met een datalek, waarbij persoonsgegevens betrokken zijn, die Ressort Wonen met bewerker heeft uitgewisseld.

C. Dit protocol wordt op de website van Ressort Wonen geplaatst.

Artikel 3 Procedure

Indien zich een datalek voordoet, worden de volgende zes fasen onderscheiden.

1. Ontdekken
2. Inventariseren
3. Beoordelen
4. Herstellen
5. Melden
6. Documenteren

1. <u>Ontdekken</u>

Wanneer een datalek wordt ontdekt, bijvoorbeeld door eigen waarneming, een klacht van een klant of een melding door een bewerker, verzamelt de betrokken ontdekker zoveel mogelijk informatie over het datalek en meldt dit direct bij Tim Huurman en Bert Hoogendonk.
Deze procedure geldt overigens ook bij bij verlies of diefstal van laptop, smartphone, iPad, USB-stick. Kortom: alles waar informatie van is af te leiden of toegang geeft tot.

De ontdekker wint zoveel mogelijk informatie over het datalek in:

- Een **concrete beschrijving** van het datalek (wat is er precies gebeurd?)
- Welke (**typen**) **persoonsgegevens** zijn gelekt?
- **Hoeveel personen** zijn betrokken bij het datalek?
- Kan de groep betrokkenen worden **beschreven**? (klant, personeel, 55+ers, asielzoekers, bijzondere doelgroep, etc.)
- Wat is de **oorzaak**?
- **Wanneer** heeft het datalek plaatsgevonden?
- Zijn er **contactgegevens van getroffen klant(en)**, zodat (eventueel) contact kan worden opgenomen?
- **Contactgegevens** van ontdekker in verband met nadere informatie.

2. <u>Inventariseren</u>

Bert beoordeelt of voldoende informatie over het datalek bekend is. Bij onvoldoende informatie zet Bert aanvullende vragen uit.

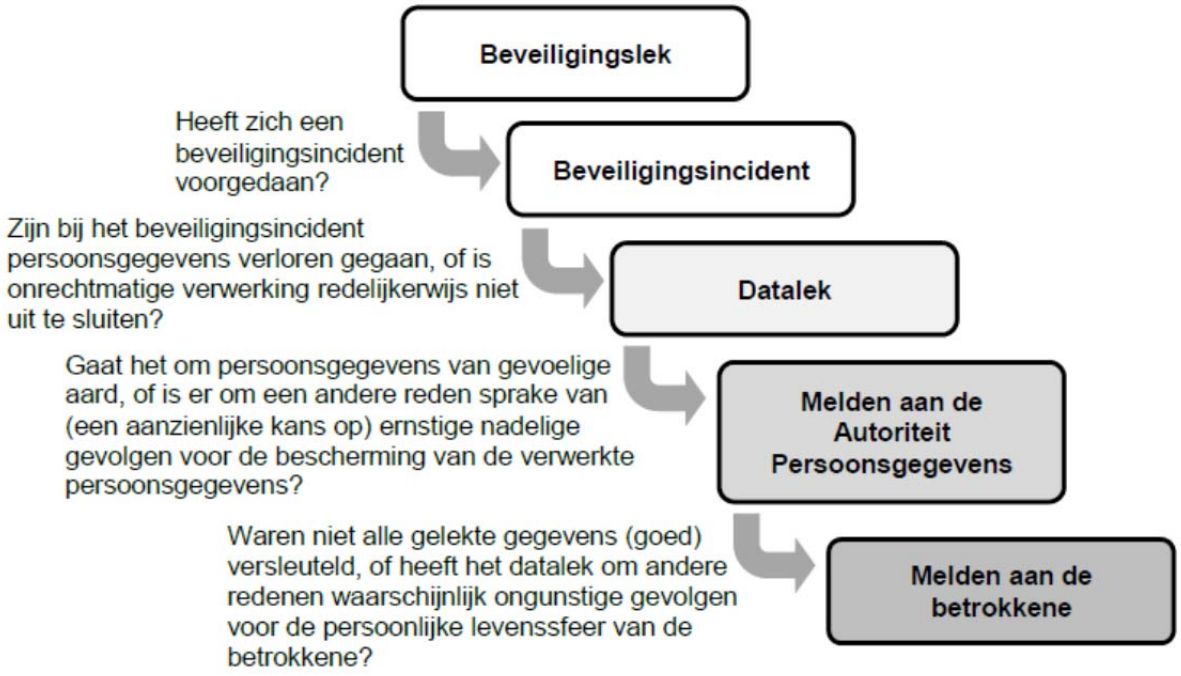
Een deel van deze informatie wordt door **ontdekker** verstrekt (zie ook meldingsformulier datalek). Een deel door de **Tim Huurman** (vanuit zijn ICT-functie). Een deel moet de **Bert Hoogendonk** zelf verkrijgen d.m.v. kwalificatie.

Samenvatting van het incident	**Mogelijke gevolgen voor de persoonlijke levenssfeer van betrokkenen**
Aantal betrokkenen bij de inbreuk	**Wordt het datalek aan betrokkenen gemeld? Hoe? Inhoud melding?**
Omschrijving van de groep betrokkenen	**Waarom wordt het lek niet aan betrokkenen gemeld?**

Datum/periode van de inbreuk	**Heeft de inbreuk betrekking op personen in andere EU landen?**
Aard van de inbreuk	**Technische en organisatorische maatregelen ter aanpak inbreuk en voorkoming verdere inbreuk**
Type persoonsgegevens in kwestie	**Zijn de gegevens onbegrijpelijk voor degenen die er kennis van kunnen hebben genomen? Hoe?**

3. Beoordelen

Wanneer de Bert voldoende informatie heeft verzameld, beoordeelt hij aan de hand van onderstaand beslismodel of een melding aan de Autoriteit Persoonsgegevens en/of betrokkenen noodzakelijk is.



(bron: Beleidsregels voor toepassing van artikel 34a van de Wbp)

De afweging om wel of niet te melden wordt genomen in overleg met de bestuurder.

Een datalek moet gemeld worden bij de Autoriteit Persoonsgegevens indien het ***leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens***.

De betrokkene moet onmiddellijk in kennis van de inbreuk wordt gesteld, indien dit ***waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.***
(Bijvoorbeeld: onrechtmatige publicatie, aantasting van eer en goede naam, (identiteits)fraude of discriminatie).

4. Herstellen

Tim achterhaalt wat de oorzaak van het lek is en zorgt ervoor dat het lek wordt hersteld.

5. Melden

a. Indien de conclusie bij stap 3 is dat er gemeld moet worden aan de Autoriteit Persoonsgegevens, dan doet de Bert dit binnen 72 uur.

b. Indien de Bert 72 uur na de ontdekking van het incident nog niet volledig zicht heeft op wat er gebeurd is en om welke persoonsgegevens het gaat, wordt de melding gedaan op basis van de gegevens waarover de Bert op dat moment beschikt. Eventueel kan Bert de melding naderhand nog aanvullen of intrekken.

c. Indien de conclusie bij stap 3 is dat gemeld moet worden aan de betrokkene(n), dan gebeurt dat op de volgende manier:
   - ***Onmiddellijk***. Het onmiddellijk melden houdt in, dat Ressort Wonen na het ontdekken van een datalek enige tijd mag nemen voor nader onderzoek.
   - De melding doet hij ***schriftelijk***.
   - De melding gebeurt zorgvuldig en “behoorlijk”, dus bijvoorbeeld niet via een algemene mail, portaal, etc. wat misschien niet doorlopend wordt bekeken.
   - Indien onduidelijk is wie de betrokkenen zijn, dient Ressort Wonen het datalek landelijk te melden in de pers.

6. <u>Documenteren</u>

a. De informatie die in de voorafgaande stappen is ingewonnen of ontstaan (bijvoorbeeld meldingsnummer, afschrift melding, brief aan betrokkenen) worden gearchiveerd door Bert.

b. Incidentoverzichten worden minimaal 5 jaar bewaard.

Artikel 4 Inwerkingtreding

Dit protocol treedt in werking op 18 juli 2017 (datum vaststelling in MT)