Protocol melding en afhandeling beveiligings- of datalek, versie 1.1 - 19 oktober 2018

1. Inleiding

De achtergrond van deze procedure is de Meldplicht datalekken. Met ingang van 1 januari 2016 is de Wet bescherming persoonsgegevens ('Wbp') aangevuld met artikel 34a Wbp.[1] Sindsdien geldt een meldplicht voor datalekken. Ook in de Algemene Verordening Gegevensbescherming ('AVG'), welke sinds 25 mei 2018 geldt, is een dergelijke meldplicht voor datalekken opgenomen. Deze meldplicht houdt in dat organisaties een datalek onverwijld moeten melden aan de Autoriteit Persoonsgegevens (AP) en in bepaalde gevallen ook aan de betrokkenen.

Dit document beschrijft de procedure die gehanteerd wordt bij (het vermoeden van) een beveiligings- of datalek binnen Bureau Buitenland.com, dan wel bij (het vermoeden van) een beveiligings- of datalek dat buiten Bureau Buitenland.com heeft plaatsgevonden maar waarvoor Bureau Buitenland.com toch de verantwoordelijkheid draagt (als verwerker dan wel verwerkingsverantwoordelijke). Deze procedure is mede gebaseerd op de 'Beleidsregels voor de toepassing van artikel 34a van de Wbp' ('Beleidsregels') van de AP.[2]

Beveiligings- of datalekken zijn incidenten rondom verwerkingen van persoonsgegevens met een potentieel grote impact. Als Bureau Buitenland.com als gevolg van een datalek een grote groep betrokkenen moet informeren kan dit hoge kosten met zich meebrengen, naast een mogelijke boete van de toezichthouder. Het snel en adequaat onderzoeken, beperken van de gevolgen, het melden en afhandelen van een datalek zijn dan ook van groot belang.

Met het volgen van deze procedure wordt het volgende resultaat nagestreefd:

- voorspelbaar zijn voor alle belanghebbenden;
- waarborgen van de belangen van Bureau Buitenland.com en de betrokkenen;
- op zorgvuldige en systematische wijze analyseren van een (mogelijk) beveiligings- of datalek;
- bevorderen van het nemen van passende verbetermaatregelen en het structureel borgen ervan.

Leeswijzer en onderhoud

De activiteiten in het protocol, bijbehorende verantwoordelijkheden en bevoegdheden worden in de volgende paragrafen stapsgewijs uitgewerkt.

Deze procedure wordt na het eerste gebruiksjaar en vervolgens 3-jaarlijks geëvalueerd door de directie van Bureau Buitenland.com en opnieuw vastgesteld.

[1] Vanaf mei 2018 is de Algemene Verordening Gegevensbescherming van toepassing. Ook onder deze wetgeving is het melden van datalekken verplicht.

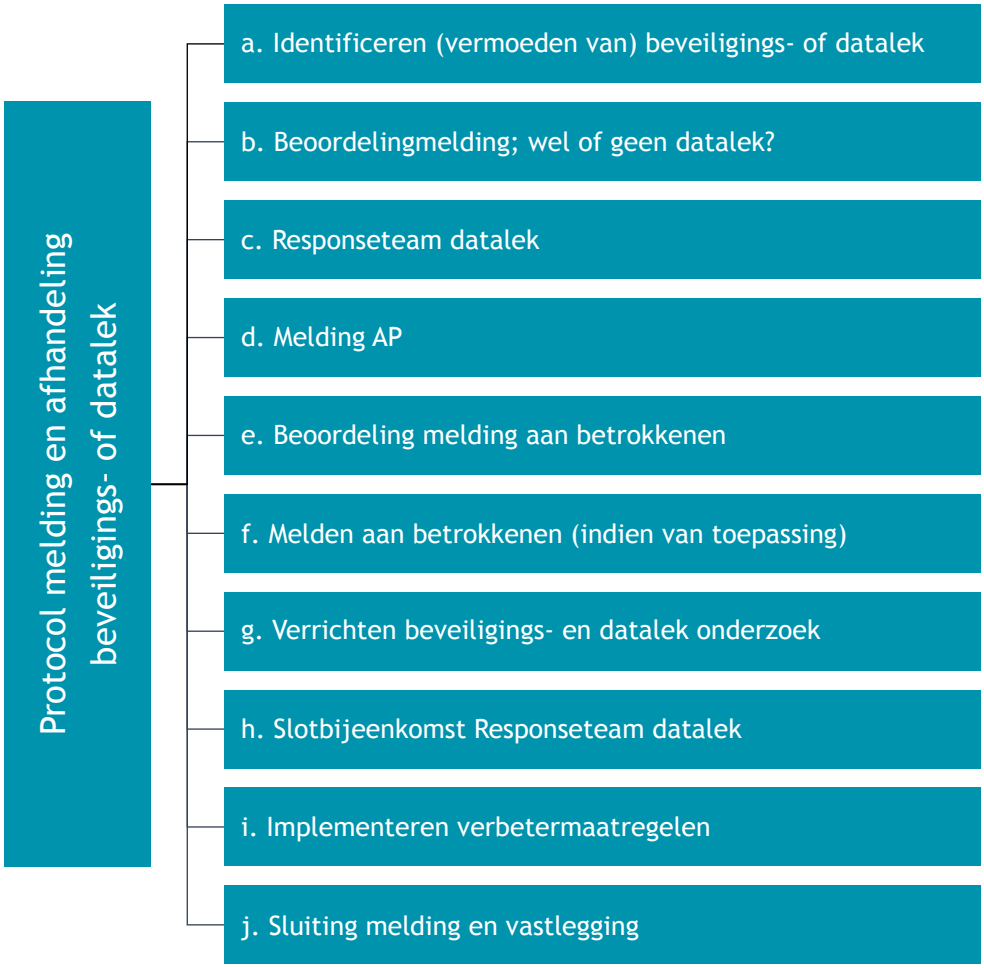
[2] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf

2. Definities[3]

- **Betrokkene**: degene op wie een persoonsgegeven betrekking heeft.
- **Datalek**: een inbreuk op de beveiliging waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking; dus blootgesteld aan datgene waartegen beveiligingsmaatregelen bescherming hadden moeten bieden.
- **Beveiligingslek**: een mogelijk beveiligingslek, waardoor de bescherming van persoonsgegevens op enig moment is doorbroken en waardoor de persoonsgegevens mogelijk zijn blootgesteld aan verlies of onrechtmatige verwerking. Het is daarbij niet van belang of de verantwoordelijke passende technische of organisatorische beschermingsmaatregelen heeft getroffen of niet. Ieder datalek is een beveiligingslek, niet ieder beveiligingslek is een datalek.
- **Persoonsgegevens**: alle gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd.
- **Response team datalekken**: het team dat zorgdraagt voor een onderzoek en over de uitkomsten rapporteert.
- **Verwerker**: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen, in dit geval Bureau Buitenland.com.
- **Verwerking van persoonsgegevens**: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens zoals bijvoorbeeld het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
- **(Verwerkings-)verantwoordelijke**: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
- **Wet**: Algemene Verordening Gegevensbescherming (“AVG”).

3. Protocol

[3] Voor zover dezelfde begrippen gelden als in het privacyreglement persoonsgegevens personeel wordt dezelfde definitie gehanteerd.



a. Identificeren van een beveiligings- of datalek
De melding van (een vermoeden) van een beveiligings- of datalek kan te allen tijde door iedereen worden gedaan, door personeelsleden van Bureau Buitenland.com, maar ook door externen binnen en buiten deze organisatie.[4] Eenieder die een (mogelijk) beveiligings- of datalek constateert, meldt dit incident per omgaande aan de directie van Bureau Buitenland.com, via sg@bureaubuitenland.com.

Het doen van de melding is vormvrij, om de drempel laag te houden. Melder hoeft enkel een zo uitgebreid mogelijke beschrijving van het beveiligings- of datalek te geven. Melder kan eventueel documenten toevoegen ter onderbouwing van de melding. De melder kan urgentie meegeven aan de melding: response binnen 15 minuten, 1 uur, een dag of een week. Dit leidt tot snellere start van de behandeling en bewaking van de voortgang.

Nadat de melding is gedaan, neemt de directie van Bureau Buitenland.com deze de melding in behandeling, waarbij een permanente bereikbaarheid middels e-mail en SMS gewaarborgd is.

De directie van Bureau Buitenland.com begint met het aanleggen van een logboek, waarin alle relevante gebeurtenissen, beslissingen en tijdstippen worden vastgelegd. Indien relevant wordt ook informatie veiliggesteld voor een eventuele juridisch vervolg van het incident.

[4] Ook een verwerker kan een (vermoeden van) een beveiligings- of datalek constateren en melden aan diens opdrachtgever binnen de organisatie.

b. Beoordeling melding; wel of geen datalek?
De directie van Bureau Buitenland.com neemt op verzoek of eigen initiatief contact op met de melder (mits de melding niet anoniem is gedaan). De directie van Bureau Buitenland.com zorgt zo spoedig mogelijk voor volledige en juiste informatie, zoals opgenomen in het meldingsformulier van AP[5] en zorgt voor een eerste analyse om te bekijken of er sprake is van een beveiligings- of datalek.

De beoordeling of er sprake is van een beveiligings- of datalek, en of er gemeld moet worden aan AP, komt tot stand op grond van de heersende wet- en regelgeving. Bij de beoordeling spelen o.a. een rol:

- is er enkel sprake van een dreiging van verlies (dus een beveiligingslek)?
- is er sprake van verlies van persoonsgegevens;
- is er sprake van onrechtmatige verwerking van persoonsgegevens;
- is er sprake van een enkele tekortkoming of kwetsbaarheid in de beveiliging;

- kan redelijkerwijs worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid;
- zijn er persoonsgegevens van gevoelige aard gelekt;

- leiden de aard en de omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen.

In het geval dat het beveiligingslek niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens is er geen sprake van een datalek maar alleen van een beveiligingslek. Melding bij AP is dan niet aan de orde, maar de melding wordt dan wel geregistreerd door de directie van Bureau Buitenland.com.

Blijkt uit de eerste analyse dat er sprake is van een (mogelijk) datalek, dan voert de directie van Bureau Buitenland.com als Responseteam Datalek onmiddellijk overleg over de te nemen stappen en acties.

c. Responseteam Datalek
Het team bestaat uit de directie van Bureau Buitenland.com.

Het Responseteam datalek draagt zorgt voor (en legt vast):

- beoordeling van de melding;
- uitvoering noodzakelijke acties met betrekking tot het datalek (bijvoorbeeld datalek onmiddellijk dichten, sporen verzamelen, toegang tot informatie beperken en eventueel hulp inroepen voor nader onderzoek);
- of en wat gemeld gaat worden bij AP;
- wijze van afhandeling intern, inclusief communicatie naar de melder, betreffende afdeling-(en) en manager(s);
- of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden;
- het al dan niet doen van aangifte en vaststellen of er sprake is van strafrechtelijke verwijtbaarheid;

- besluiten over in-en externe communicatie: op welk moment, door welke actiehouder en welke boodschap;
- op welke wijze er intern wordt gerapporteerd;
- of eventuele schade is gedekt door de verzekeringspolis.

d. Melding AP
De directie van Bureau Buitenland.com verzorgt, indien er sprake is van een datalek dat gemeld moet worden bij AP, tijdig (onverwijld, zonder onnodige vertraging, en zo mogelijk

5 https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?1

niet later dan 72 uur na de ontdekking van het datalek) de elektronische melding bij AP[6] .
De directie van Bureau Buitenland.com registreert de ontvangstbevestiging van AP en slaan het meldingsformulier op. De directie van Bureau Buitenland.com fungeert als contactpersoon inzake de communicatie met AP.

e. Beoordeling melding aan betrokkenen
Indien een datalek is gemeld aan AP dient tevens vastgesteld te worden of het datalek ook moeten worden gemeld aan degenen om wiens gegevens het gaat (betrokkenen).

f. Melden aan betrokkenen (indien van toepassing)
Indien een datalek moet worden gemeld aan betrokken, stelt de directie van Bureau Buitenland.com een kennisgeving aan betrokkenen op.

De melding bevat in ieder geval de aard van de inbreuk, contactgegevens van Bureau Buitenland.com, het informatiepunt waar de betrokkenen meer informatie over de inbreuk kan krijgen en de maatregelen die de organisatie aanbeveelt aan de betrokkenen om te nemen teneinde de negatieve gevolgen van de inbreuk te beperken.

g. Verrichten datalek onderzoek
De directie van Bureau Buitenland.com stelt een onderzoek in naar de feitelijke toedracht van het datalek en onderzoekt of en zo ja hoe dergelijke datalekken in de toekomst voorkomen kunnen worden.

De bevoegdheden van de directie van Bureau Buitenland.com zijn:

- vrijheid om met alle partijen betrokken bij het datalek en de melding te spreken;
- alle relevant geachte documenten & data inzien en bewaren;
- toegang tot alle plaatsen die nodig geacht worden ten behoeve van een zorgvuldige analyse;
- actie naar verwerkers conform afspraken in de toepasselijke verwerkersovereenkomst;
- het recht en de middelen om externe deskundigen in te zetten in het onderzoek.

h. Slotbijeenkomst Responseteam datalek
Zo snel als mogelijk presenteert de directie van Bureau Buitenland.com de bevindingen & aanbevelingen en besluiten daarop:

- welke verbetermaatregelen getroffen moeten worden;
- of en hoe over het rapport en de aanbevelingen gecommuniceerd wordt.

i. Implementeren verbetermaatregelen
De directie van Bureau Buitenland.com is ook verantwoordelijk voor de implementatie van de vanuit het beveiligings- of datalek vastgestelde verbetermaatregelen. De directie ziet toe op de communicatie rondom de verbetermaatregelen en dat de genomen maatregelen worden geëvalueerd op effectiviteit.

j. Sluiting melding en vastlegging
De directie van Bureau Buitenland.com informeert de direct bij het incident betrokken personen op het moment dat het datalek definitief afgehandeld is en de melding gesloten is.

Het datalek wordt opgenomen in het logboek datalekken.

---

6 https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?1

Aldus vastgesteld door directie BureauBuitenland, op 19 oktober 2018 te Helmond.