



Datalekken bij grootschalige postverzending

23 februari 2017

Inleiding

Een aantal organisaties op wie de meldplicht datalekken van toepassing is verzendt grote aantallen poststukken met daarin gevoelige persoonsgegevens. Het gaat hier onder meer om banken, verzekeringsmaatschappijen en pensioenfondsen. Deze organisaties spannen zich in om te zorgen dat deze poststukken bij de juiste ontvanger terecht komen. Desondanks komt een klein deel van de poststukken bij een verkeerde ontvanger terecht, of wordt geopend geretourneerd, of komt nooit aan. Deze incidenten vallen onder de meldplicht datalekken en moeten in ieder geval worden gemeld aan de Autoriteit Persoonsgegevens en indien van toepassing ook aan de betrokkene.

Onder bepaalde voorwaarden is het mogelijk om datalekken bij grootschalige postverzending in bulk te melden aan de Autoriteit Persoonsgegevens. Het vervolg van dit document gaat hier nader op in.

De Autoriteit Persoonsgegevens stelt deze mogelijkheid in eerste instantie gericht open voor organisaties die zijn aangesloten bij de Pensioenfederatie, het Verbond van Verzekeraars, de Nederlandse Vereniging van Banken alsmede voor een beperkt aantal andere organisaties. Na een proefperiode zal de Autoriteit besluiten om de mogelijkheid om datalekken bij grootschalige postverzending in bulk te melden eventueel breder open te stellen. U zult hierover nader worden geïnformeerd via onze website.

Welke incidenten kan ik in bulk melden?

Het gaat om poststukken met gevoelige gegevens die bij grootschalige postverzending bij de verkeerde ontvanger terecht komen (en die door die ontvanger ook worden geopend), of die geopend worden geretourneerd, of die nooit aankomen. De mogelijkheid om in bulk te melden geldt voor individuele poststukken en niet voor, bijvoorbeeld, een complete zending poststukken die door een derde ergens wordt aangetroffen.

Onder welke voorwaarden kan ik incidenten in bulk melden?

Voor het in bulk melden van datalekken gelden de volgende voorwaarden:

- Het in bulk melden van datalekken gebeurt door een specifieke functionaris binnen de organisatie. Als de organisatie beschikt over een functionaris voor de gegevensbescherming of een privacyfunctionaris ligt het voor de hand om deze taak bij hem of haar te beleggen.
- De functionaris die is belast met het doen van de bulkmeldingen beschikt over een overzicht van alle incidenten die in bulk zijn gemeld.
- Bij alle incidenten die in een bulkmelding worden gemeld gaat het om poststukken die inhoudelijk vergelijkbaar zijn, zodat gegevens zoals de aard van de persoonsgegevens en de mogelijke gevolgen voor de betrokkenen in de melding correct kunnen worden weergegeven.
- De incidenten waarom het gaat worden uiterlijk op de overeenkomstige dag van de eerstvolgende kalendermaand na de dag van ontdekking gemeld aan de Autoriteit Persoonsgegevens.



- De hierboven weergegeven regeling is alleen bedoeld voor verantwoordelijken voor wie het melden van ieder vermist of geopend retour ontvangen poststuk een onredelijke administratieve last betekent. Bij constatering van misbruik zal de Autoriteit Persoonsgegevens in eerste instantie de verantwoordelijke waarschuwen en eventueel handhavend optreden.
- Ook in andere situaties waar bijvoorbeeld het aantal of de aard van de meldingen daar aanleiding toe geeft, kan de Autoriteit voor één of meer verantwoordelijken de mogelijkheid beëindigen om datalekken in bulk te melden.

Hoe doe ik een bulkmelding?

Voor de bulkmelding gebruikt u het elektronische formulier op onze website.¹ Dit zelfde formulier kunt u ook gebruiken om de melding aan te vullen of in te trekken.

Bij het doen van een bulkmelding vult u het formulier in zoals u dat bij een normale datalekmelding zou doen, met de volgende aandachtspunten:

- Bij de gegevens van de contactpersoon vult u de gegevens in van de functionaris die binnen uw organisatie is belast met het doen van de bulkmeldingen.
- Onder 'Gegevens over het datalek' geeft u bij de samenvatting aan dat het gaat om een bulkmelding van poststukken die bij de verkeerde ontvanger terecht zijn gekomen, die geopend zijn geretourneerd of die nooit zijn aangekomen.
- De vraag 'Is bekend wanneer de inbreuk was?' beantwoordt u met 'Ja'.
- De vraag 'Is de exacte datum bekend wanneer de inbreuk was?' beantwoordt u met 'Nee'.
- Bij 'Exacte datum waarop de inbreuk was' vult u niets in.
- Bij 'Startdatum van de periode waarbinnen de inbreuk was' vult u de datum in waarop de betreffende zending poststukken is verzonden.
- Bij 'Einddatum van de periode waarbinnen de inbreuk was' vult u de einddatum in van de periode waarop de bulkmelding betrekking heeft.
- Bij 'Wanneer werd de inbreuk ontdekt?' vult u de datum in waarop u het eerste poststuk waarop de melding betrekking heeft geopend retour ontving, of de datum waarop u voor het ontdekte dat een van de poststukken waarop de melding betrekking heeft bij de verkeerde ontvanger terecht was gekomen of niet was aangekomen.

Kan ik na 25 mei 2018 nog steeds incidenten in bulk melden?

De mogelijkheid tot het doen van bulkmeldingen die in dit document wordt beschreven gaat uit van de huidige meldplicht voor datalekken die is opgenomen in de Wet bescherming persoonsgegevens (Wbp). De Wbp is de Nederlandse privacywet. Per 25 mei 2018 is de algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum nog maar één privacywet geldt in de hele Europese Unie (EU). De Wbp geldt dan niet meer. Ook de AVG kent een meldplicht voor datalekken, die per 25 mei 2018 dus gaat gelden in de gehele EU. De Autoriteit Persoonsgegevens zal in de komende periode onderzoeken wat de gewijzigde privacywetgeving betekent voor de mogelijkheid om datalekken in bulk te melden. Als dit leidt tot aanpassingen, of tot beëindiging van de mogelijkheid om bulkmeldingen te doen, dan wordt u daarover via onze website nader geïnformeerd.

¹ datalekken.autoriteitpersoonsgegevens.nl.