SWV ZUID HOLLAND WEST

Samenwerkingsverband Zuid-Holland West

Protocol Datalekken

Versie: maart 2019

Inleiding

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens.

Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.

Protocol datalekken

Dit protocol voorziet op een gestructureerde wijze in het melden van datalekken in het kader van de Algemene Verordening Gegevensbescherming (AVG).

Daarnaast is een schema opgenomen om te beoordelen of een datalek gemeld moet worden aan de Autoriteit Persoonsgegevens dan wel aan de betrokkene.

Een datalek hoeft alleen gemeld te worden bij de Autoriteit Persoonsgegevens als dit leidt tot ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens. Of als een aanzienlijke kans bestaat dat dit gebeurt.

Betrokkenen hoeven alleen geïnformeerd te worden als dit datalek waarschijnlijk ongunstige gevolgen heeft voor hun persoonlijke levenssfeer.

Een datalek moet bij de Autoriteit Persoonsgegevens worden gemeld via het meldloket datalekken:

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken .

Voor wie geldt dit protocol?

Dit protocol geldt voor alle medewerkers van het Samenwerkingsverband Zuid-Holland West die in het kader van hun functie gegevens van leerlingen, hun ouders en/of medewerkers bewerken.

Taken, verantwoordelijkheden en bevoegdheden

1. Iedere medewerker die direct of indirect kennis draagt of krijgt van een incident inzake het lekken van privacygegevens, is verplicht dit direct te melden aan de directeur.
2. De directeur en de systeembeheerder zijn verantwoordelijk voor het onderzoeken van het incident.
3. De directeur is verantwoordelijk voor de beoordeling van het datalek en bij een meldplichtige datalek voor het doen, aanvullen en intrekken van de meldingen van datalekken bij de Autoriteit Persoonsgegevens.
4. De systeembeheerder is verantwoordelijk voor het ondernemen van preventieve en repressieve acties, daarbij worden de aanwijzingen van de directeur in acht genomen.
5. Het bevoegd gezag is samen met de directeur verantwoordelijk voor de actualiteit van deze procedure.

Uitvoering

1. De medewerker die direct of indirect kennis draagt, of krijgt van een incident inzake het lekken van privacygegevens meldt dit direct aan de directeur en de systeembeheerder. De melding wordt gedaan via de e-mail, onder vermelding van ‘datalekken’.
2. De directeur, in samenwerking met de systeembeheerder en de functionaris gegevensbescherming (FG), onderzoekt het incident. Hierbij is aandacht voor de volgende aspecten:
    a. wat is de aard van het datalek;
    b. wat is de oorzaak dat dit incident heeft plaatsgevonden;
    c. is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures;
    d. is de organisatie verwijtbaar;
    e. van het incident wordt een verslag gemaakt.

3. Als er is vastgesteld dat er sprake is van een meldplichtige datalek doet de directeur een melding van het datalek aan de Autoriteit Persoonsgegevens.
4. De directeur onderhoudt contact met de Autoriteit Persoonsgegevens over de melding datalekken. Eventuele aanwijzingen van de Autoriteit Persoonsgegevens worden vastgelegd en opgevolgd.

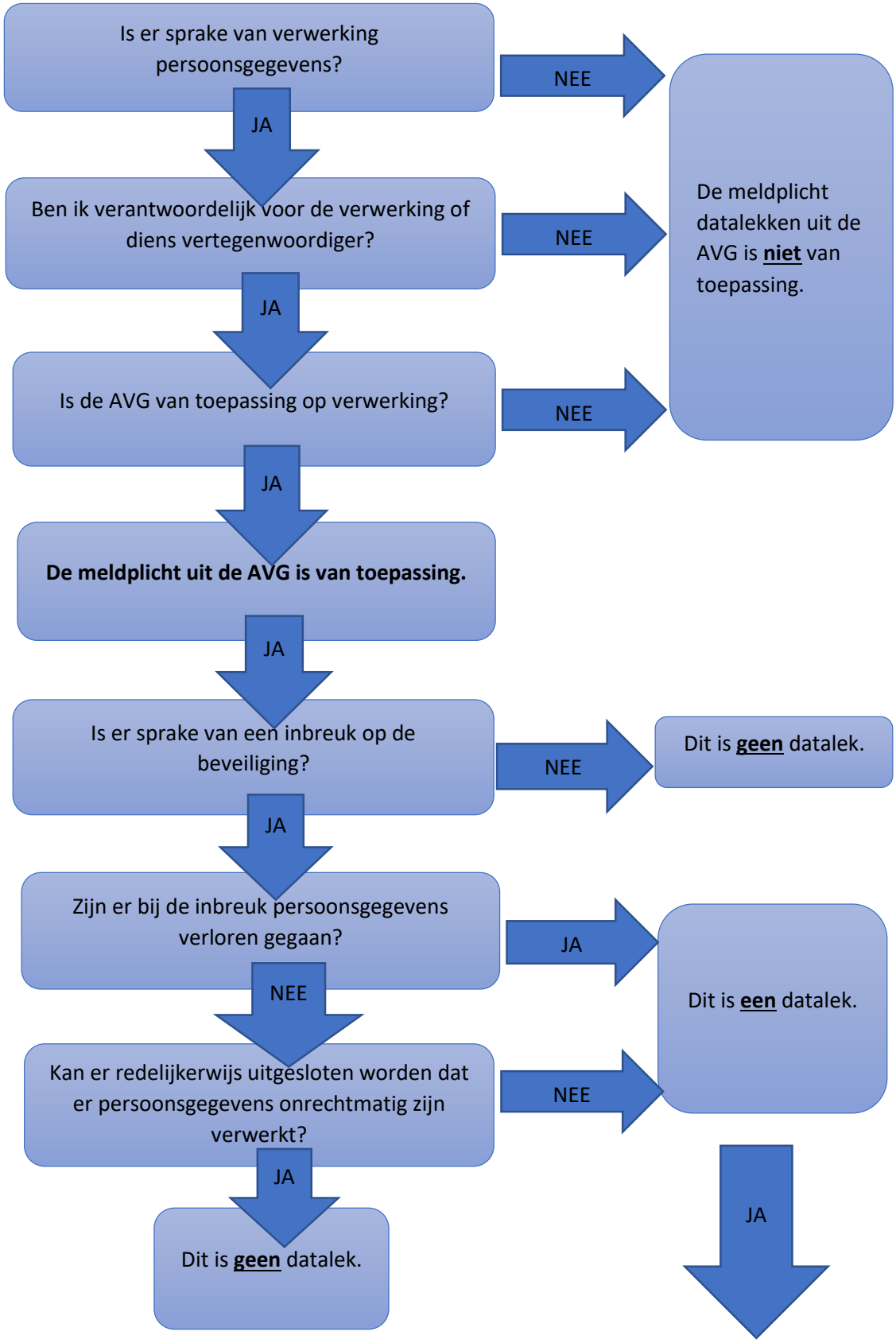
Interne controle

1. Op basis van de gedurende een jaar ontvangen meldingen analyseert het bevoegd gezag, samen met de directeur, met de FG en de systeembeheerder, deze en stellen een verbeterplan of -advies op. Dit plan of advies wordt opgenomen in de jaarlijks uit te brengen bestuursverslag;
2. Minimaal jaarlijks beoordeelt het bevoegd gezag of de procedure en de uitvoering nog met elkaar in overeenstemming zijn. Indien deze niet met elkaar overeenkomen wordt beoordeeld of de procedure geactualiseerd moet worden of dat medewerkers geïnstrueerd moeten worden op een juiste toepassing van de procedure.

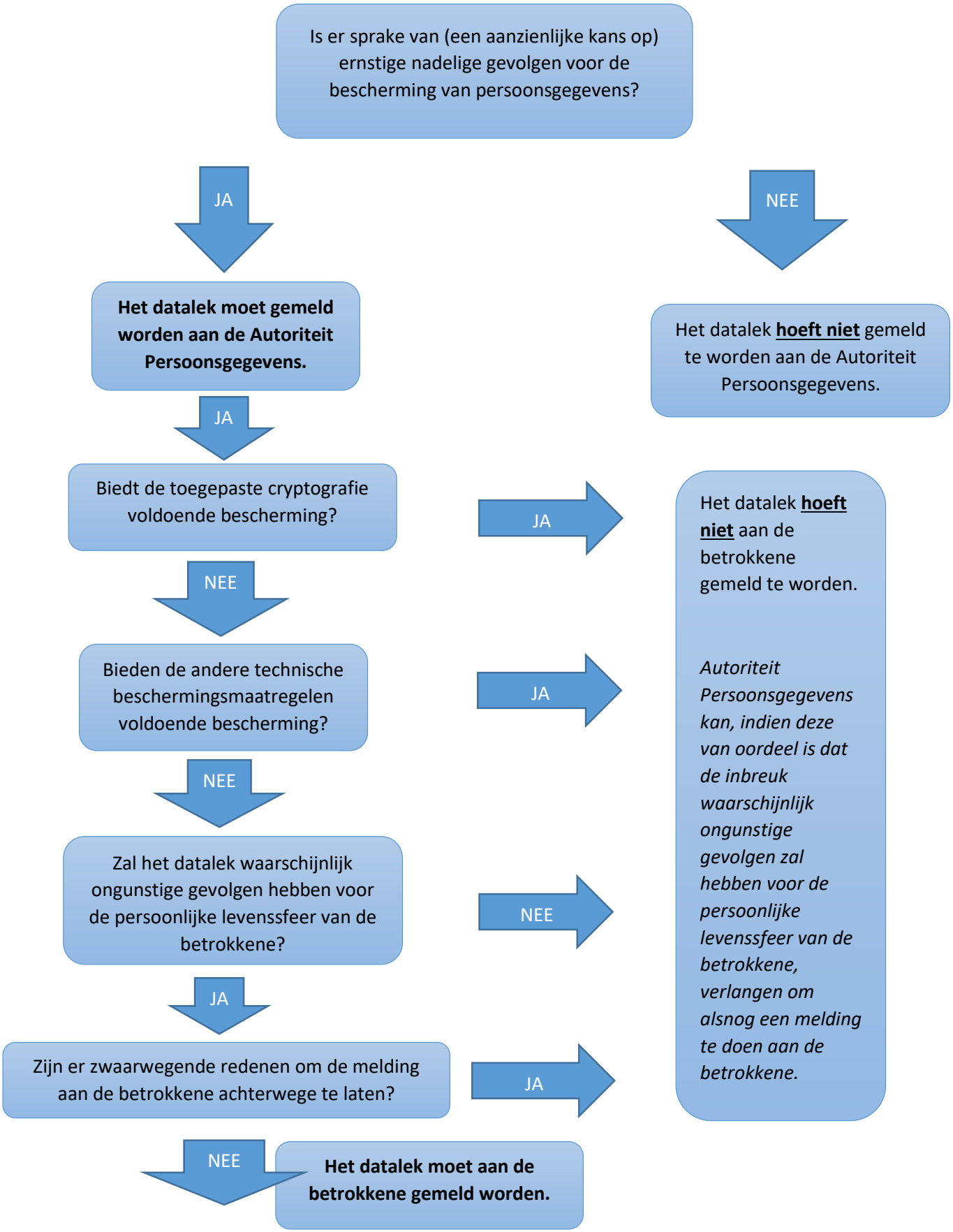
Schema beoordeling datalek

Onderstaand schema geeft aan hoe een datalek wordt beoordeeld en of deze gemeld moet worden aan de Autoriteit Persoonsgegevens en/of de betrokkene. De stappen in het schema worden altijd doorlopen. Hiervan wordt een verslag gemaakt.

Stroomschema protocol melding datalekken SWVZHW



Vervolg stroomschema protocol melding datalekken SWVZHW



Mededeling aan de Autoriteit Persoonsgegevens

Bij een datalek dient in ieder geval de volgende informatie gemeld te worden aan de Autoriteit Persoonsgegevens:

- Aard en omvang van de breuk;
- Waar mogelijk de categorieën van de betrokkenen, de persoongegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
- De naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- De waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegeven;
- De maatregelen die SWVZHW heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelinge gevolgen daarvan.

Mededeling aan de betrokkenen

Wanneer betrokkenen geinformeerd moeten worden over de inbreuk, dient die kennisgeving in ieder geval de volgende elementen te bevatten:

- Een omschrijving van de aard van de breuk;
- De naam en contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- De waarschijnlijke gevolgen van de inbreuk voor betrokkenen;
- De maatregelen die het SWVZHW heeft voorgesteld of genomen om de breuk aan te pakken, waaronder de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Documentatie

SWVZHW zal de datalekken documenteren in een overzicht van datalekken die zich hebben voorgedaan. In dit overzicht worden de feiten omtrent de breuk en de gevolgen hiervan gedocumenteerd. Ook de corrigerende maatregelen worden hierbij vastgelegd. De volgende tabel illustreert de manier waarop datalekken vastgelegd zullen worden.

Datum datalek:	Feitelijke gebeurtenissen:	Gevolgen voor de betrokkenen:	Corrigerende maatregelen: