n o t i t i e

Kenmerk	[redacted]	Van	[redacted]
			[redacted]
Datum	9 juli 2018	Aan	[redacted]
Onderwerp	Procedure datalekken		

Voorstel

De procedure datalekken van 29 mei 2017 is geactualiseerd op basis van de nieuwe beleidsregels van de Autoriteit Persoonsgegevens. Voorgesteld wordt deze aangepaste versie vast te stellen en te implementeren.

Toelichting op voorstel

Vanaf 2016 zijn organisaties verplicht een ernstig lek van persoonsgegevens direct te melden bij de Autoriteit Persoonsgegevens (AP, voorheen het College bescherming persoonsgegevens), dat is de nationale toezichthouder. Binnen de GGD Zeeland dient ieder vermoeden van een datalek gemeld te worden via de knop Gegevensbescherming op Insite. Daarna dient, door de DPO's (functionaris gegevensbescherming), de afweging gemaakt te worden of het datalek ook gemeld dient te worden aan de AP en/of personen van wie de persoonsgegevens zijn gelekt. Deze meldplicht voor inbreuken op beveiligingsmaatregelen voor persoonsgegevens is bij wet ingevoerd als aanvulling op de Wet bescherming persoonsgegevens (Wbp). 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 Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

Het doel van de meldplicht is om de gevolgen van een datalek voor de betrokkenen zoveel mogelijk te beperken en zodoende een bijdrage te leveren aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens. Als er geen melding wordt gemaakt van een datalek kan dit bestraft worden met een bestuurlijke boete van de AP.

Meer dan 70% van alle security incidenten wordt mede veroorzaakt door onwetendheid en onjuist handelen van eigen medewerkers. Mensen klikken op links in Phishing Mails, verliezen USB-sticks en delen -bewust of onbewust- informatie met ongeautoriseerde personen via e-mail of onveilige cloud oplossingen, zoals Dropbox. Medewerkers zijn zich vaak niet bewust van hun rol op het gebied van informatiebeveiliging binnen de organisatie.

Toepassingsgebied

Deze aangepaste procedure beschrijft hoe te handelen binnen de GGD, indien er sprake is van een datalek of wanneer een datalek vermoed wordt. De meldplicht is eveneens van toepassing op de GGD, als het datalek bij een derde is ontstaan, bijvoorbeeld een bewerker van persoonsgegevens van de GGD. Deze procedure is mede gebaseerd op de beleidsregels van de Autoriteit Persoonsgegevens (AP) inzake de meldplicht datalekken in de Wet bescherming persoonsgegevens.

Doel

Het doel van deze procedure is vast te leggen, welke stappen genomen moeten worden door de GGD Zeeland bij het vermoeden van of kennis nemen van een incident dat (mogelijk) aangemerkt kan worden als een datalek. Het volgende resultaat wordt hiermee nagestreefd:

- het steeds volgen van een eenduidige procedure;
- het zorgvuldig waarborgen van de belangen van de GGD, het individu dan wel een ander bedrijf dat betrokken is bij het incident, zijnde (mogelijk) datalek;
- het op zorgvuldige en systematische wijze analyseren van een incident, zijnde mogelijk datalek, zodat aanwezige risicomomenten in het proces zichtbaar worden. Centraal staat hierbij het vaststellen van de onvolkomenheden in de (toepassing van) technische en organisatorische beveiligingsmaatregelen, die (mogelijk) hebben kunnen leiden tot het incident;
- het bevorderen van het nemen van passende verbetermaatregelen en het structureel borgen van deze verbetermaatregelen;
- het realiseren van een voldoende en eenduidige interne en op verzoek externe verantwoording over de afhandeling van een incident, zijnde (mogelijk) datalek.

Afkortingen en Begrippen

AP: Autoriteit persoonsgegevens. De toezichthouder op de WbP (en straks AVG) in Nederland. (Zie website Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl)

AVG: Algemene Verordening Gegevensbescherming. De nieuwe Europese Privacy Wetgeving die per 25 mei 2018 van toepassing zal zijn en verder gaat dan de huidige WbP.

DPO: Data Protection Officer, of in het Nederlands ook wel Functionaris Gegevensbescherming (FG). Deze persoon houdt zich bezig met de naleving van de privacy wetgeving in een bedrijf of instelling. Met de komst van de AVG is een benoeming van deze functionaris vanaf 25 mei 2018 verplicht.

ISO: Information Security Officer. Deze persoon houdt zich bezig met het adviseren en coördineren bij de verdere ontwikkeling en uitrol van informatieveiligheid.

WBP: Wet Bescherming Persoonsgegevens. De nationale wetgeving die gebaseerd is op de Europese privacy richtlijn uit 1995 en die opgevolgd wordt door de AVG

Incident m.b.t. gegevensbescherming:
Een mogelijk beveiligingsincident, waardoor de bescherming van persoonsgegevens op enig moment is doorbroken en waardoor de persoonsgegevens 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 incident, niet ieder incident is een datalek.

Datalek:
Een inbreuk op de beveiliging (zoals bedoeld in artikel 4, punt 12, AVG) waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking; dus blootgesteld aan datgene waartegen beveiligingsmaatregelen (artikel 5, punt f, AVG) bescherming moesten bieden

Let Op! Er is sprake van een datalek als persoonsgegevens verloren raken of onrechtmatige verwerking redelijkerwijs niet kan worden uitgesloten. Onder onrechtmatige verwerking valt onder andere het aanpassen en/of veranderen van persoonsgegevens en niet geautoriseerde toegang tot deze persoonsgegevens. Er is dus niet alleen sprake van een datalek bij een inbraak door een hacker.

Rollen
Functionaris gegevensbescherming: [redacted]
ISO: [redacted]

Registratie
Zowel een incident m.b.t. gegevensbescherming of een datalek wordt direct mondeling gemeld bij een van de ISO's en DPO's en binnen 3 werkdagen geregistreerd via de knop Informatieveiligheid op Insite. De verantwoordelijken voor afhandeling: Information Security Officer (ISO) en Data Protection Officer (DPO, zgn. Functionaris Gegevensbescherming).

Te registreren relevante zaken, o.a.:

- adresgegevens, telefoonnummer, medische gegevens, enz.).
- Vanuit welke gegevensbron zat de gelekte gegevens/informatie.
- Op welke gegevensdrager, zoals een laptop, telefoon, usb-stick, enz.
- Wanneer het datalek ontdekt is *(het systeem registreert automatisch de meldingsdatum)*
- Waardoor zijn de gegevens gelekt (diefstal, gegevens zijn zoekgeraakt)
- Zijn het gegevens waarvan de GGD Zeeland verantwoordelijk c.q. eigenaar is?
- Zo nee, van welke organisatie zijn de gegevens dan wel

Mondelinge meldingen worden direct door de ISO's en DPO's opgepakt en afgehandeld. Na registratie worden tevens workflowtaken opgestart via Insite.

Werkwijze

De werkwijze vindt plaats volgens onderstaande volgorde.

1. Analyse

Beide ISO's stellen zich op de hoogte van de eerste feiten, dat wil zeggen een eerste check of het gaat om een beveiligingsincident of een beveiligingsincident met persoonsgegevens. Na afstemming met de DPO's, stellen de ISO's indien nodig een onderzoek in en delen deze bevindingen met de DPO's.

2. Informeren en organiseren

De DPO's informeren de manager BB en/of de directeur. Indien nodig worden andere belanghebbenden op de hoogte gebracht. In afstemming wordt bepaald wie bij elkaar geroepen dient te worden voor een impactanalyse. Het beveiligingsincident kan reden geven om direct onderhoud te plegen of direct een wijziging door te voeren in de systemen.

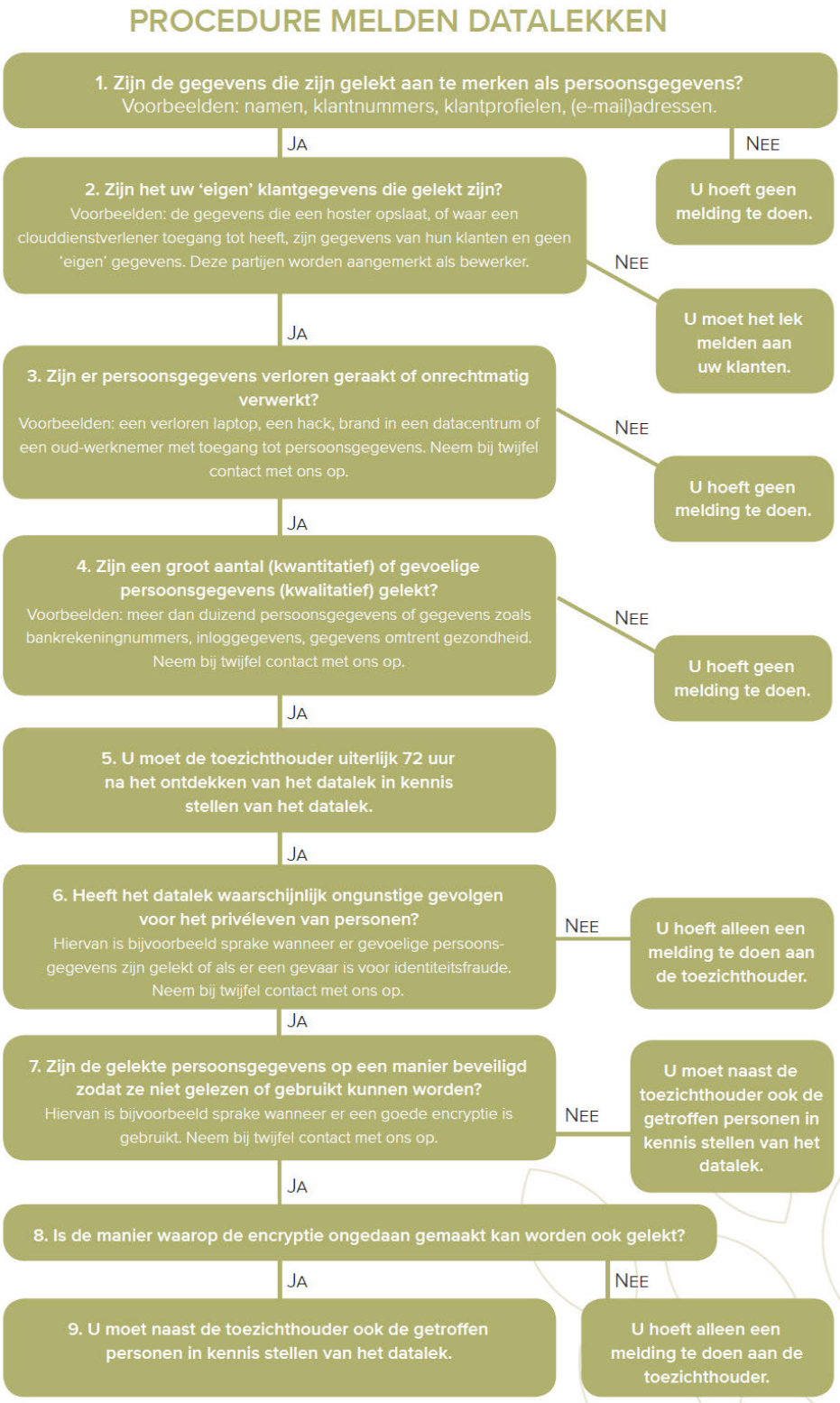
3. Impactanalyse

De DPO's en ISO's voeren een impactanalyse uit.

- Wie wordt/worden er door geraakt?
- Is het een ernstig datalek dat bij de AP gemeld moet worden?

De Autoriteit Persoonsgegevens (AP) heeft beleidsregels opgesteld om organisaties te helpen bij het bepalen of sprake is van een datalek dat zij moeten melden bij de AP en eventueel aan de betrokkenen. Zie onderstaande schema's.

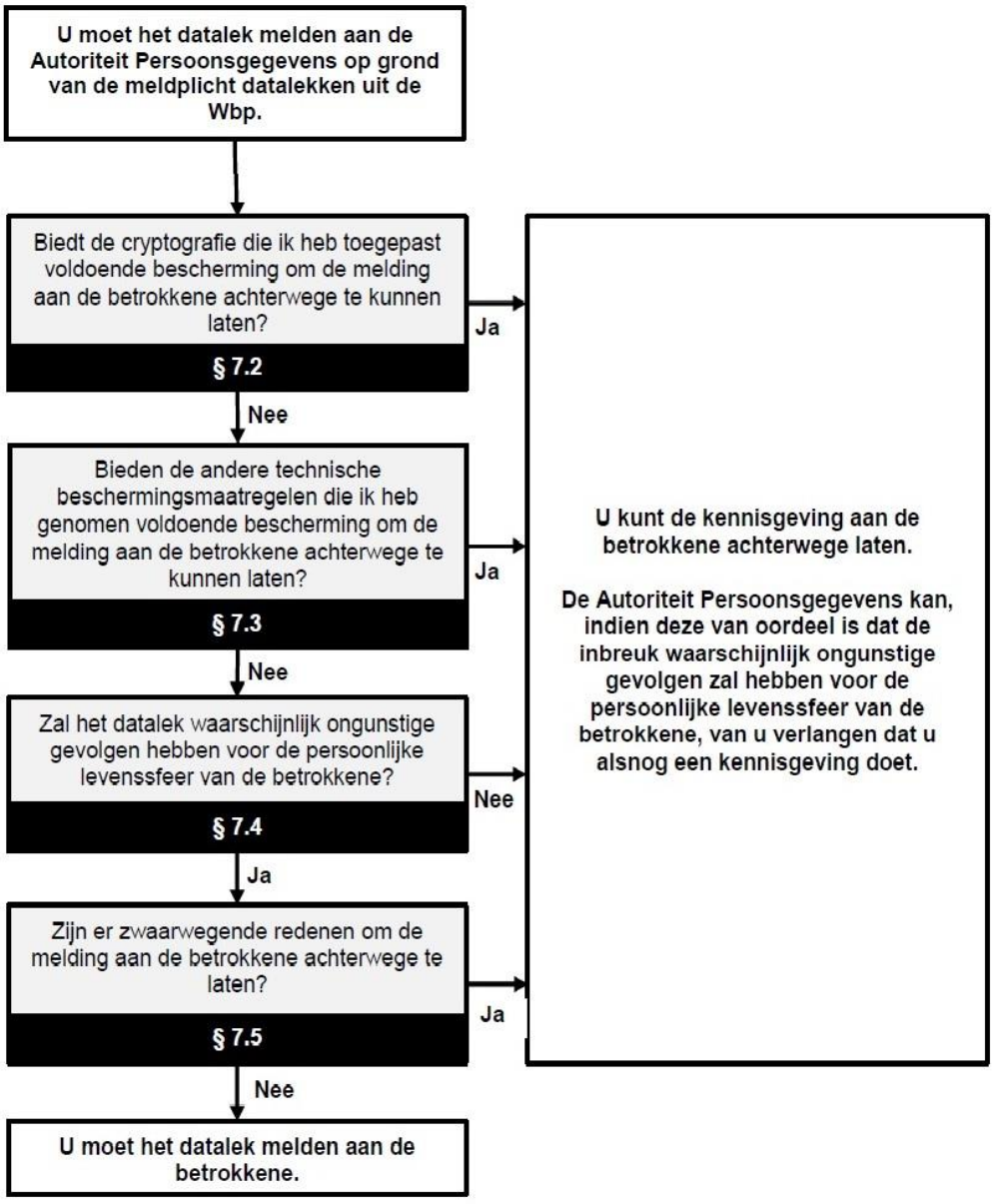
Het onderstaande schema wordt gehanteerd om het antwoord op die vraag te bepalen zodat er wel of niet gemeld dient te worden naar de AP.



Bron

https://ictrecht.nl/content/uploads/2017/05/Factsheet-Impact-van-de-Meldplicht-Datalekken-ICTRecht.pdf

4. Moet het datalek gemeld worden aan betrokkene(n)?



Bron:https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken_wbp.pdf

5. Communicatie

De DPO's zijn verantwoordelijk voor de communicatie: de DPO's informeren alle belanghebbenden, te weten de directie, de *Autoriteit Persoonsgegevens (AP)*, alle getroffenen. De DPO's bepalen in afstemming met de directeur of de AP geïnformeerd dient te worden. Dit kan door middel van een formulier op de website, zie https://datalekken.autoriteitpersoonsgegevens.nl

6. Evaluatie

De werkgroep gegevensbescherming evalueert en stelt indien nodig een of meer maatregelen voor ter voorkoming van een dergelijk incident. De uitkomst van de evaluatie en aanbevelingen wordt gedeeld met de manager bedrijfsbureau en de directeur. Indien nodig worden aanbevelingen opgevolgd en gecommuniceerd naar alle betrokkenen.

7. Afsluiting

De melding op Insite wordt gesloten, nadat de melding is bijgewerkt met informatie over de behandeling van het datalek: welke betrokkenen zijn geïnformeerd, welke maatregelen zijn genomen.

8. Jaarlijks verslag

De werkgroep gegevensbescherming maakt een jaaranalyse van alle gemelde incidenten m.b.t. privacy- en gegevensbescherming inclusief datalekken en brengen daarover schriftelijk verslag uit.

Datum	Vergadering	Besluit	Vervangt notitie nr:
9 juli 2018		Vastgesteld	