PerspektieV
Leren door ervaren

PROTOCOL WET DATALEKKEN

PerspektieV
Leren door ervaren

Inhoudsopgave

I Inleiding

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

Rechten van betrokkenen:

1. Inzagerecht
2. Recht op informatie
3. Kopie van gegevens opvragen
4. Correctie of aanvulling van gegevens
5. Verwijdering van persoonsgegevens
6. Recht op dataportabiliteit
7. Bezwaar maken tegen gebruik

A Doel protocol

Het doel is dat beveiligingsincidenten en datalekken volgens de geldende wet-/regelgeving wordt geregistreerd en/of gemeld. Daarnaast moet het leiden tot het direct opheffen van het incident om verdere schade zoveel mogelijk te voorkomen.

B Toepassingsgebied

<u>Onder beveiligingsincidenten wordt verstaan:</u>
Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. We hoeven dan geen melding te doen aan de Autoriteit Persoonsgegevens. Niet ieder beveiligingsincident is een datalek.

<u>Onder een datalek wordt verstaan;</u>
Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident moet je bijvoorbeeld denken aan het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker. Als er persoonsgegevens van gevoelige aard zijn gelekt is over het algemeen een melding noodzakelijk (zie bijlage 1).

C Revisiebeheer

Revisie datum	Wijziging	Vastgesteld door
01-07-2019	Eerste versie	Directie
15-02-2021	Nieuw logo toegevoegd.	Directie

D Evaluatie

Evaluatiedatum
15-02-2022

E Externe richtlijnen en bronnen

1	**Wettelijk kader**	Algemene Verordening Gegevensbescherming Meldplicht datalekken Beleidsregels meldplicht datalekken (2015) Privacystatement formulier meldplicht datalekken (AP) Europese richtlijn melden datalek 3 oktober 2017 Concept Cybersecuritywet
2	**Richtlijn**	ISO/NEN 27002 NEN 7510 PRISMA-methodiek

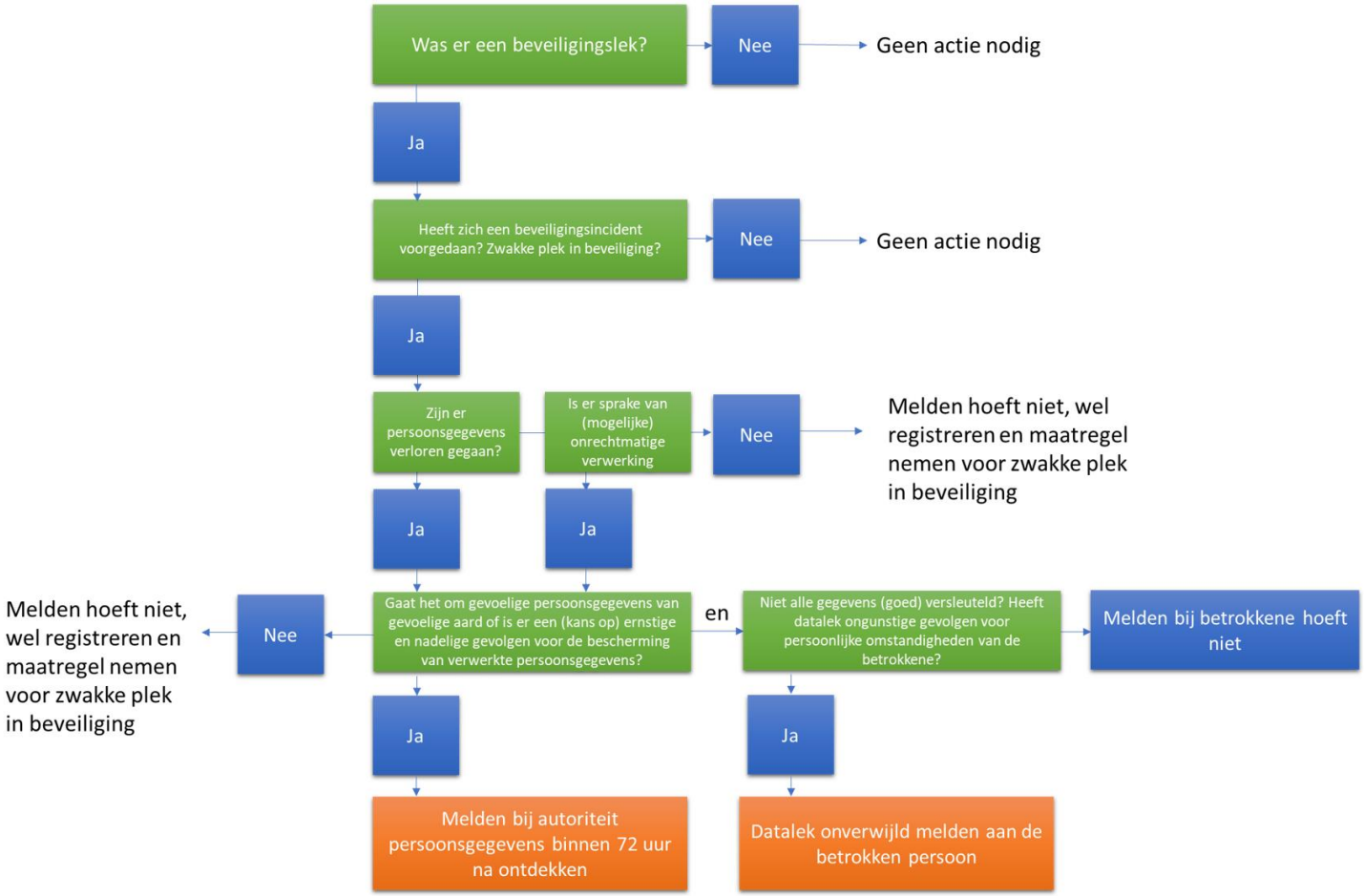
F Bijbehorende documenten

1	**Bijbehorende documenten**	B02 Beveiligingsbeleid NEN 7510 en opvolgend REGL-101 Privacyreglement
2	**Formulieren**	n.v.t.
3	**Registraties**	Incidentenoverzicht privacy

G Hulpmiddelen

n.v.t.

II Protocol datalekken



Artikel 1 Algemene bepalingen

1.1	De directie heeft de kaders voor het melden van datalekken vastgelegd in het **B02 Beveiligingsbeleid.**
1.2	De directie legt risico's vast in alle procedures en processen van het kwaliteitssysteem.
1.3	De directie heeft tijdens het inwerkprogramma aandacht voor incidenten en datalekken.

Artikel 2 Ontstaan incident

2.1	Tijdens het ontstaan van een incident neemt de betrokken medewerker direct maatregelen om erger te voorkomen. Indien nodig worden hulpdiensten ingeschakeld. De maatregelen zijn afhankelijk van de ernst van het incident en kent de volgende classificatie; ▪ **Laag**: geen schade ▪ **Middel**: geringe problemen of geringe operationele ongemakken ▪ **Hoog**: kortdurende en significante impact op de operationele of tactische doelstellingen ▪ **Zeer hoog**: ernstige impact op betrokkenen of de strategische lange termijn doelstellingen of brengt het voortbestaan van de organisatie in gevaar.
2.2	De betrokken medewerker meldt het incident mondeling bij de directie. Indien van toepassing geeft de directie aanwijzingen over direct te nemen maatregelen. De betrokken medewerker vult een incidentformulier in en dit wordt geregistreerd op het overzicht **Excel-E12 Incidentenoverzicht privacy.**
2.3	Afhankelijk van het type incidenten (beveiligingsincident of datalek) worden vervolgacties ondernomen; ▪ Directe maatregelen: om de gevolgen te beperken. ▪ Beveiligingsincident; corrigerende maatregel om zwakte in beveiliging op te heffen ▪ Datalek: afhankelijk van de ernst wordt binnen 72 uur na ontdekken een melding gedaan bij de Autoriteit Persoonsgegevens en indien verplicht aan de directbetrokkene (degene van wie de gegevens gelekt zijn. ▪ **Meldloket**: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0
2.4	Registraties worden maandelijks geëvalueerd door de directie: ▪ het incident wordt besproken en er wordt bepaald of het incident juist is afgehandeld ; ▪ indien nodig worden corrigerende maatregelen ingezet.

Artikel 3 Melden datalek

3.1	Vanuit de Meldplicht zijn we verplicht datalekken te melden binnen 72 uur na constateren bij de Autoriteit Persoonsgegevens. Wanneer er een hoog risico is voor cliënten moet dit onverwijld gemeld worden. Datalekken en beveiligingsincidenten (als het alleen gaat om een zwakke plek in de beveiliging) worden geregistreerd op het overzicht **Excel-E13 Overzicht bedrijfsmiddelen privacy**.
3.2	Melden aan de betrokkene doen we op het moment dat een datalek ongunstige gevolgen heeft voor de betrokkene en diens persoonlijke levenssfeer (zie bijlage 1): - Door het verlies, onrechtmatig gebruik of misbruik kunnen belangen geschaad worden: ▪ Onrechtmatige publicatie ▪ Aantasting in eer en goede naam ▪ (identiteits)fraude ▪ Discriminatie ▪ Persoonsgegevens van gevoelige aard.

Artikel 4 Vaststellen en wijziging protocol

4.1	Dit protocol is vastgesteld op 15-02-2021 door de directie.
4.2	In alle gevallen waarin dit protocol niet voorziet beslist de directie.

Bijlage 1 Persoonsgegevens van gevoelige aard

Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

- Gegevens over de financiële of economische situatie van de betrokkene
- Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salarissen betalingsgegevens.
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene
- Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- Gebruikersnamen, wachtwoorden en andere inloggegevens
- De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude
- Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (BSN).