Protocol datalekken
Samenwerkingsverband Roosendaal e.o.

.

Geactualiseerd 22-12-2023
Vastgesteld door bestuur op 8 januari 2024
Versie 4.0

Inhoud

Inleiding

Met ingang van 1 januari 2016 geldt de meldplicht datalekken uit de Algemene Verordening Gegevensbescherming (AVG). De Functionaris Gegevensbescherming (FG-CED groep) houdt toezicht op de verwerking van persoonsgegevens. Bij een datalek zal hij, indien nodig, een melding doen bij de Autoriteit Persoonsgegevens.

Het swv ROOS vo heeft naast de ingehuurde FG van de CED groep een eigen contactpersoon Privacy Officer (PO) die indien nodig een melding doet bij de FG van de CED groep. De rol van de PO binnen swv ROOS vo wordt vervuld door de stafmedewerker kwaliteit.

Dit protocol beschrijft wanneer er sprake is van een datalek en of er ook een melding moet worden gedaan aan de FG-CED groep. Vervolgens bepaald de FG-CED groep of ook melding gemaakt moet worden bij de Autoriteit Persoonsgegevens.

In het protocol wordt men aan de hand van 7 vragen begeleid hoe om te gaan met het voorgevallen incident:

1. Is de meldplicht datalekken van toepassing?
2. Is een gebeurtenis te beschouwen als een datalek?
3. Moet het datalek gemeld worden?
4. Hoe en wanneer moet het datalek worden gemeld?
5. Moet het datalek ook worden gemeld aan de betrokkene?
6. Hoe en wanneer moet het datalek worden gemeld aan de betrokkene?
7. Welke gegevens moeten worden gearchiveerd?

Begrippenlijst

a. Autoriteit Persoonsgegevens: zelfstandig bestuursorgaan dat bij wet als toezichthouder is aangesteld voor het toezicht op de correcte verwerking van persoonsgegevens, voorheen het College bescherming persoonsgegevens;

b. AVG: Algemene Verordening Gegevensbescherming, een Europese verordening die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert;

c. Bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;

d. Betrokkene: degene op wie een persoonsgegeven betrekking heeft;

e. Bindende aanwijzing: de zelfstandige last die de Autoriteit wegens een overtreding wordt opgelegd;

f. Datalek: beveiligingsinbreuk zoals bedoeld in artikel 33 AVG;

g. Functionaris Gegevensbescherming: persoon, werkzaam bij de CED groep, die is belast met de controle op de naleving van de bepalingen uit de Wbp en datalekken moet melden bij de Autoriteit Persoonsgegevens; (FG-CED groep)

h. Privacy Officer (PO): intern aanspreekpunt belast met de controle op de naleving van de bepalingen uit de AVG innen het swv en datalekken moet melden bij de FG-CED groep.

i. Ontvanger: degene aan wie persoonsgegevens worden verstrekt;

j. Persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare persoon, zoals bedoeld in artikel 4, lid 1 AVG;

k. Persoonsgegevens van gevoelige aard: persoonsgegevens zoals bedoeld in artikel 9 AVG;

l. Verantwoordelijke: degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking vaststelt. Het inschakelen van derden maakt hier geen uitzondering op;

m. Verwerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt;

n. Verwerking: verwerking van persoonsgegevens zoals bedoeld in artikel 4 lid 2 AVG;

1. Is de meldplicht datalekken uit de AVG van toepassing?

Dat is het geval indien:

a) Er sprake is van verwerking van persoonsgegevens. De verwerking van persoonsgegevens betreft elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, zoals het verzamelen, vastleggen, ordenen, raadplegen en verspreiden.
b) swv ROOS vo is de verantwoordelijke of diens vertegenwoordiger.
c) De AVG op de verwerking van toepassing is. Bepaalde verwerkingen vallen door hun aard of doelstelling buiten de reikwijdte van de AVG. In beginsel is op de verwerking van persoonsgegevens binnen Roos VO altijd de AVG van toepassing.

2. Is een gebeurtenis te beschouwen als een datalek?

Als de gebeurtenis valt onder de werking van de AVG komt men toe aan vraag 2: is er sprake van een datalek?

Dit is het geval indien:

d) Er sprake is van een inbreuk op de beveiliging. Dat wil zeggen dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan.

EN

e) Bij de inbreuk persoonsgegevens verloren zijn gegaan of redelijkerwijs niet kan worden uitgesloten dat er persoonsgegevens onrechtmatig zijn verwerkt, waaronder moet worden begrepen de aantasting van de persoonsgegevens, onbevoegde kennisneming, wijziging of verstrekking daarvan.

3. Moet het datalek gemeld worden?

Een datalek moet gemeld worden aan de Privacy Officer (PO). Dit kan via meldpuntprivacy@swvroosvo.nl. Het is belangrijk om bij melding altijd de direct leidinggevende te CC-en.

De Privacy Officer neemt bij een melding contact op met de FG-CED groep en informeert de directeur-bestuurder van swv ROOS vo. “Iedere inbreuk in verband met persoonsgegevens” moet worden gemeld bij de AP tenzij niet waarschijnlijk is dat deze een risico inhoudt.

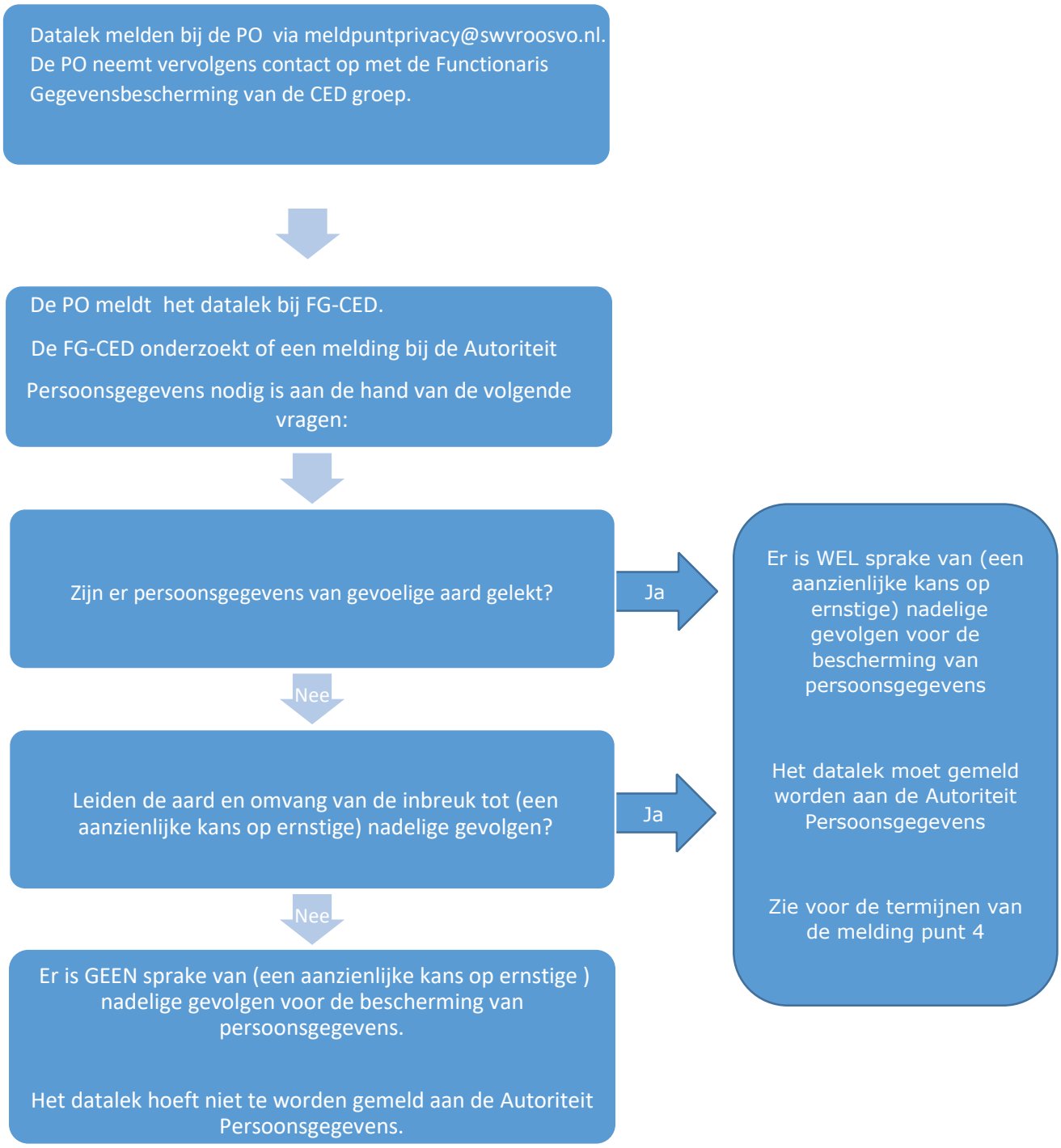
Er is sprake van een (aanzienlijke) inbreuk als één van de volgende situaties aan de orde is;

- Persoonsgegevens van gevoelige aard zijn gelekt, namelijk:
- Bijzondere persoonsgegevens zoals:
  - Betreffende iemands levensovertuiging of godsdienst, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging;
  - Strafrechtelijke persoonsgegevens; en
  - Persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag;

OF

- Persoonsgegevens die anderszins van gevoelige aard zijn, waaronder:
  - Gegevens over de financiële of economische situatie van de betrokkene;
  - Gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
  - Gebruikersnamen, wachtwoorden en andere inloggegevens;
  - Gegevens die kunnen worden misbruikt voor (identiteits-)fraude;
  - Gegevens uit DNS (domain name system)-databanken, gegevens waar een bijzondere wettelijke bepaalde geheimhoudingsplicht op rust en gegevens die onder een beroepsgeheim vallen.

- De aard en omvang van de inbreuk leiden tot (een aanzienlijke kans op) ernstige nadelige gevolgen. Hierbij is van belang:
- Gaat het om veel persoonsgegevens per persoon of om gegevens van grote groepen?
- Zijn de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpend?
- Worden de persoonsgegevens binnen ketens gedeeld?
- Gaat het om persoonsgegevens van kwetsbare groepen?


Datalek melden bij de PO via meldpuntprivacy@swvroosvo.nl.
De PO neemt vervolgens contact op met de Functionaris Gegevensbescherming van de CED groep.
De PO meldt het datalek bij FG-CED.
De FG-CED onderzoekt of een melding bij de Autoriteit Persoonsgegevens nodig is aan de hand van de volgende vragen:
Zijn er persoonsgegevens van gevoelige aard gelekt?
Ja
Nee
Leiden de aard en omvang van de inbreuk tot (een aanzienlijke kans op ernstige) nadelige gevolgen?
Ja
Nee
Er is GEEN sprake van (een aanzienlijke kans op ernstige) nadelige gevolgen voor de bescherming van persoonsgegevens.
Het datalek hoeft niet te worden gemeld aan de Autoriteit Persoonsgegevens.
Er is WEL sprake van (een aanzienlijke kans op ernstige) nadelige gevolgen voor de bescherming van persoonsgegevens
Het datalek moet gemeld worden aan de Autoriteit Persoonsgegevens
Zie voor de termijnen van de melding punt 4

4. Hoe en wanneer moet het datalek worden gemeld?

Als er het vermoeden is van een datalek moet dit gemeld worden zoals bepaald onder 3. Het is noodzakelijk om de melding te doen binnen de daarvoor geldende termijnen:

Termijn
Een datalek moet onverwijld worden gemeld. Dit houdt in dat de verantwoordelijke na het ontdekken van een mogelijk datalek enige tijd mag nemen voor nader onderzoek. Op deze manier kunnen de voorgaande stappen uit dit protocol worden doorlopen en kunnen onnodige meldingen worden voorkomen.

De termijn voor het melden begint te lopen op het moment dat de verantwoordelijke of een bewerker op de hoogte raakt van een incident dat mogelijk onder de meldplicht datalekken valt. De melding vindt uiterlijk binnen 72 uur na de ontdekking van het datalek plaats bij de toezichthouder van swv ROOS vo en de Autoriteit Persoonsgegeven door de FG-CED groep. Uiteraard alleen als er sprake is van een datalek en het onder de meldplicht datalekken valt.

De melding
Zodra binnen het swv ROOS vo een mogelijk datalek is geconstateerd wordt er onverwijld (binnen 12 uur) contact opgenomen met de PO. De PO meldt dit binnen 12 uur aan de FG-CED groep. De FG-CED groep beoordeelt (nogmaals) of er sprake is van een datalek vallend onder de werking van de meldplicht datalekken uit de AVG. Indien hier sprake van is wordt de toezichthouder geïnformeerd en vindt er een melding plaats bij de Autoriteit Persoonsgegevens. De leidinggevende van het swv ROOS vo moet eveneens direct worden ingelicht.

Aangifte
Indien er sprake is van een datalek kan er een vermoeden zijn van strafbaar handelen. Zo is bijvoorbeeld hacken strafbaar gesteld. In die gevallen moet er behalve een melding datalekken bij de FG-CED groep, ook aangifte worden gedaan bij de politie. Een afschrift hiervan moet worden gezonden aan de directeur-bestuurder van swv ROOS vo en de Privacy Officer.

5. Moet het datalek worden gemeld aan degene van wie de persoonsgegevens zijn gelekt?

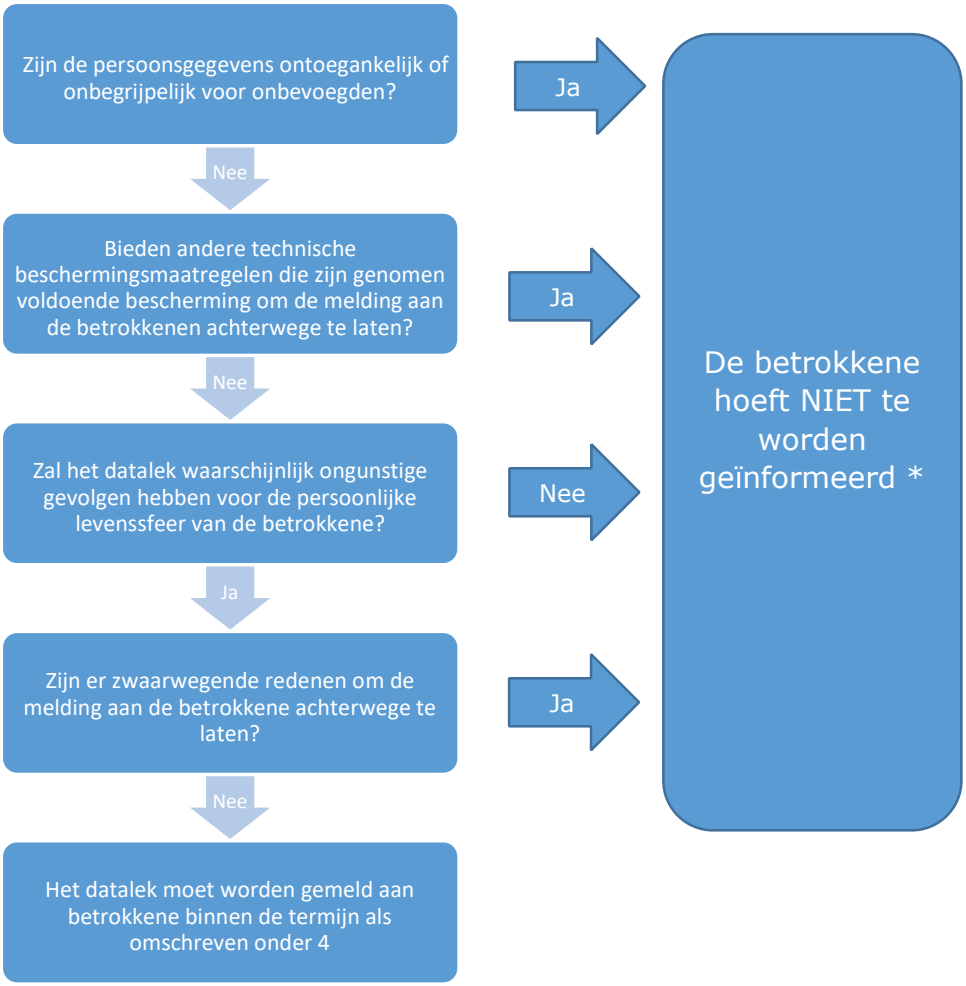
Het uitgangspunt is dat indien er persoonsgegevens zijn gelekt die waarschijnlijk een hoog risico inhouden (art 34 AVG) dit wordt gemeld aan degene wiens persoonsgegevens het betreft.

Het datalek hoeft niet te worden gemeld aan de betrokkene indien één van de volgende situaties zich voordoet:

a. Er zijn passende technische beschermingsmaatregelen genomen waardoor de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens, bijvoorbeeld door adequate encryptie[1] en hashing[2].
b. Andere technische beschermingsmaatregelen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten, bijvoorbeeld door een tijdige en adequate remote wiping[3] en pseudonimisering[4].
c. Het is onwaarschijnlijk dat het datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene. Indien persoonsgegevens van gevoelige aard zijn gelekt, moet het altijd gemeld worden.
d. Er zijn andere zwaarwegende redenen om de melding aan de betrokkene achterwege te laten.

In een stroomschema ziet het er als volgt uit:

[1] Versleuteling
[2] Het omzetten van gegevens in een unieke code
[3] Het op afstand wissen van de gegevens die op een apparaat staan
[4] Technische maatregelen om te voorkomen dat de persoonsgegevens worden gekoppeld aan de oorspronkelijke identiteit van de betrokkene.



*De Autoriteit Persoonsgegevens kan, indien zij van oordeel is dat de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, verlangen om alsnog een kennisgeving aan betrokkene(n) te doen. Ook al zou dat op basis van het stroomschema niet hoeven.

Termijnen omschreven onder 4:
1) Een mogelijk datalek is geconstateerd, er wordt onverwijld (**binnen 12 uur**) contact opgenomen met de PO. De PO meldt dit binnen 12 uur aan de FG-CED groep. De FG-CED groep beoordeelt (nogmaals) of er sprake is van een datalek vallend onder de werking van de meldplicht datalekken uit de AVG. Indien hier sprake van is verzorgt de FG-CED groep een melding bij de Autoriteit Persoonsgegevens. De toezichthouder en de leidinggevende van het swv ROOS vo moeten eveneens direct worden ingelicht.

2a) Een incident dat mogelijk onder de meldplicht datalekken valt. De melding **vindt uiterlijk binnen 72 uur** na de ontdekking van het datalek plaats bij de Autoriteit Persoonsgegeven door de FG-CED groep.

2b) Indien er sprake is van een datalek kan er een vermoeden zijn van strafbaar handelen. Zo is bijvoorbeeld hacken strafbaar gesteld. In die gevallen moet er behalve een melding datalekken bij de FG-CED groep, ook aangifte worden gedaan bij de politie. Een afschrift hiervan moet worden gezonden aan de directeur-bestuurder van swv ROOS vo en de Privacy Officer.

6. Hoe en wanneer moet de melding worden gedaan aan de betrokkene?

Termijn
Een datalek moet onverwijld worden gemeld. Dat houdt in dat de verantwoordelijke, na het ontdekken van een mogelijk datalek enige tijd mag nemen voor nader onderzoek zodat betrokkene op een behoorlijke en zorgvuldige manier kan worden geïnformeerd.
De betrokkene wordt in ieder geval onmiddellijk geïnformeerd nadat er een melding bij de Autoriteit Persoonsgegevens is gedaan.

Melding
De Privacy Officer doet de melding aan de betrokkene (in overleg met de FG-CED groep). In de kennisgeving aan de betrokkene staat in ieder geval het volgende vermeld:
De aard van de inbreuk;
De contactgegevens van de Privacy Officer; en
De maatregelen die zijn aanbevolen om de negatieve gevolgen van de inbreuk te beperken.

7. Welke gegevens moeten worden gearchiveerd?

De FG-CED groep houdt een overzicht bij van alle datalekken die onder de meldplicht vallen en dus gemeld zijn aan de Autoriteit Persoonsgegevens. Per datalek bevat het overzicht in ieder geval de gegevens omtrent de aard van de inbreuk en, indien aan de betrokkene is gemeld, de tekst van de kennisgeving.