Beleid en procedure beveiligingsincidenten en datalekken

Bron

Bibliotheek PrivacyPeople

Datum	*Actie*	*Geleding*	
13-11-2021	Instemming	GMR	
14-11-2021	Vaststelling	CvB	
Gepubliceerd op website en in personeelshandboek (RAP)			

Inhoud

1 Inleiding 4

2 Definities 4

3 Wanneer is er sprake van een datalek? 5

4 Is het waarschijnlijk dat de inbreuk een risico inhoudt voor de rechten en vrijheden van betrokkenen? 6

5 Bepalingen voor de verwerker 6

6 Hoe moet een datalek gemeld worden? 7

6.1 Melding aan de AP 7

6.2 Melding aan de FG 7

6.3 Melding aan betrokkene. 7

7 Registratie bijhouden van beveiligingsincidenten c.q. datalekken 7

8 Interne procedure 7

8.1 Constateren van een mogelijk datalek door medewerker en interne melding 7

8.2 Quick Response Team 8

8.2.1 Afweging datalek 8

8.2.2 Direct te treffen maatregelen 8

8.3 Meldplicht 9

8.3.1 Melding aan Autoriteit Persoonsgegevens 9

8.3.2 Melding aan betrokkene 9

8.3.3 Leren van datalekken 9

Bijlage 1 11

Bijlage 2 13

Bijlage 3 14

1 Inleiding

In dit beleidsdocument wordt de meldplicht die Stichting Groeisaam Primair Onderwijs (in het vervolg Groeisaam genoemd) heeft in het kader van artikel 33 en 34 AVG uitgewerkt. Groeisaam is in de zin van de AVG 'verwerkingsverantwoordelijke' voor de verwerking van persoonsgegevens. Groeisaam is derhalve verplicht datalekken onverwijld te melden aan de Autoriteit Persoonsgegevens (hierna 'AP') en in bepaalde gevallen ook aan betrokkene(n). De betrokkene is degene wiens persoonsgegevens zijn gelekt.

In dit document staat beschreven hoe Groeisaam omgaat met datalekken en wanneer een datalek vanuit Groeisaam wordt gemeld aan de Autoriteit Persoonsgegevens. De meldplicht is eveneens van toepassing als het datalek bij een derde is ontstaan, bijvoorbeeld bij een verwerker van persoonsgegevens van Groeisaam. Voor verwerkers geldt dat indien zij geconfronteerd worden met een datalek, zij dit onverwijld aan de vertegenwoordiger van Groeisaam (privacycoördinator) moeten doorgeven, zodat deze namens Groeisaam de melding kan doen.

Dit beleid is gebaseerd op artikel 33 en 34 van de AVG en de 'richtsnoeren datalekken'[1] van de AP. Artikel 33 en 34 van de AVG zijn opgenomen als Bijlage 1.
Een persoonsgegeven is elk gegeven over een geïdentificeerde of identificeerbare persoon. In het geval van Groeisaam gaat het om leerlinggegevens, gegevens van ouders/verzorgers en gegevens van medewerkers.
Groeisaam verwerkt persoonsgegevens zowel digitaal als fysiek. Zodoende ontstaan risico's als mogelijk verlies en/of ongeautoriseerde toegang. Als er sprake is van een dergelijke situatie, is dit een incident en gelden er specifieke verantwoordelijkheden en handelswijzen.
Persoonsgegevens moeten adequaat beveiligd worden op organisatorisch en technisch niveau. In het informatiebeveiligingsbeleid van Groeisaam staat beschreven wat de beveiligingsnormen zijn. Dit gaat van simpele normen (*geen inlog en password in de omgeving van de werkplek achterlaten, of een collega laten inloggen met jouw gegevens*) tot ingewikkeld (*bijvoorbeeld de encryptie van gegevens bij uitwisseling over de mail*). Adequate beveiliging levert een belangrijke bijdrage aan het voorkomen van datalekken.

2 Definities

De volgende definities worden gehanteerd:

- **AP:** Autoriteit Persoonsgegevens.
- **Bestand:** Elk gestructureerd geheel van persoonsgegevens (*op papier of digitaal 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 (artikel 4 sub 6 AVG).
- **Betrokkene:** Degene op wie een persoonsgegeven betrekking heeft (artikel 4 sub 1 AVG).
- **Beveiligingsincident:** Een inbreuk op de beveiliging (zoals bedoeld in artikel 33 AVG) waarbij persoonsgegevens niet worden blootgesteld aan verlies of onrechtmatige verwerking; er is dan geen sprake van een datalek.
- **Verwerker:** Degene die ten behoeve van Groeisaam (als verwerkingsverantwoordelijke) persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen (artikel 4 sub 8 AVG: 'verwerker').
- **Datalek:** Een inbreuk op de beveiliging (zoals bedoeld in artikel 33 AVG) waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking; dus blootgesteld aan datgene waartegen beveiligingsmaatregelen (artikel 24 AVG) bescherming moesten bieden. LET OP: een incident is alleen een datalek indien het waarschijnlijk is dat de

1 Zie: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf

inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van betrokkenen. Met andere woorden: de inbreuk leidt tot diefstal, verlies of misbruik van persoonsgegevens.

- **Derden:** De bij het incident betrokken externe partij, anders dan betrokkene. Bijvoorbeeld een verwerker van persoonsgegevens t.b.v. Groeisaam (artikel 4 sub 10 AVG).
- **FG:** Functionaris Gegevensbescherming, onafhankelijke externe toezichthouder (artikel 37 AVG)
- **AVG:** General Data Protection Regulation, welke verordening geldt per 25 mei 2018.
- **Incident:** 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 (zie: Datalek).
- **Persoonsgegeven:** Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4 sub 1 AVG).
- **Quick Response Team:** Dit is het interne team binnen Groeisaam om een incident te onderzoeken alsmede hieraan opvolging te geven. Het Quick Response Team heeft de regie over het afhandelen van het incident en zorgt voor nakoming van alle wettelijke verplichtingen.
- **Verantwoordelijke:** De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4 sub 7 AVG: 'verwerkingsverantwoordelijke'). In dit geval: Groeisaam.
- **Verwerking van persoonsgegevens:** Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 4 sub 2 AVG).

3 Wanneer is er sprake van een datalek?

Allereerst moet er sprake zijn van een 'inbreuk op de beveiliging'. Indien de volgende feiten zich voordoen, is dit een inbreuk:

- De verwerkte persoonsgegevens of bestanden zijn blootgesteld aan verlies of onrechtmatige verwerking, en
- Er kan niet redelijkerwijs uitgesloten worden dat er persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt.

Verlies houdt in dat de gegevens er niet meer zijn (*er is bijvoorbeeld geen back-up beschikbaar*). Onder onrechtmatige verwerking wordt verstaan de aantasting van de gegevens, onbevoegde kennisneming, wijziging of verstrekking daarvan.
Van een datalek is mogelijk sprake indien:

- een USB-stick kwijtraakt[2];
- een laptop wordt gestolen;
- een hacker inbreekt in het systeem;
- een email wordt verzonden waarin email adressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden;

2 Bij alle voorbeelden geldt dat dit alleen een datalek is als redelijkerwijs niet kan worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid. Indien een USB-stick zwaar beveiligd is en absoluut kan worden uitgesloten dat de data op de stick onbenaderbaar is, geldt het verlies niet als een datalek, tenzij de gegevens op de stick niet elders zijn opgeslagen. Dan is het namelijk 'verlies van persoonsgegevens'.

- een malware besmetting;
- een calamiteit, zoals een brand in een datacentrum.

Ook fysieke documenten vallen onder het begrip datalek. Dit betekent dat in open ruimtes nagegaan moet worden of gegevens goed zijn afgeschermd. Denk hierbij aan openstaande kasten met gevoelige gegevens of privacygevoelige informatie die bij een kopieerapparaat blijft liggen.
Als redelijkerwijs niet kan worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid, moet het datalek aan de AP gemeld worden. LET OP: een beveiligingsincident is alleen een datalek als wordt voldaan aan de voorwaarden zoals gesteld in hoofdstuk 4.
In Bijlage 3 is een stappenplan opgenomen dat het wel/niet melden schematisch weergeeft.

4 Is het waarschijnlijk dat de inbreuk een risico inhoudt voor de rechten en vrijheden van betrokkenen?

Alleen in het geval **dat het waarschijnlijk is** dat de inbreuk een risico inhoudt voor de rechten en vrijheden van betrokkenen, hoeft er een melding plaats te vinden van een datalek aan de AP.
Hiervan is sprake in de volgende gevallen:

- Indien er persoonsgegevens van gevoelige aard gelekt zijn (i*ndien het gaat om medische gegevens, BSN, legitimatie, inloggegevens en wachtwoorden alsmede financiële gegevens wordt aangenomen dat dit meestal het geval is*), en/of
- De aard en omvang van de inbreuk leidt tot (een aanzienlijke kans op) ernstige nadelige gevolgen. De AVG omschrijft dit als: ‘een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.’ Dit houdt in dat er bijvoorbeeld sprake is van (mogelijke) discriminatie, financiële schade, reputatierisico en/of identiteitsfraude.

Indien medische gegevens zijn ingezien door (*zelfs interne*) onbevoegden is er sprake van een datalek. Financiële gegevens en BSN-nummer zijn gevoelig met het oog op (identiteits)fraude.
Een melding hoeft niet te worden gedaan als het **NIET** waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van betrokkenen.

5 Bepalingen voor de verwerker

Voor verwerkers geldt dat indien zij geconfronteerd worden met een datalek, zij dit onverwijld aan de vertegenwoordiger van Groeisaam moeten doorgeven, zodat deze namens Groeisaam de melding kan doen.
Een verwerker verwerkt persoonsgegevens ten behoeve van de verantwoordelijke (i.c. Groeisaam), enkel en alleen op instructie van de verantwoordelijke. De verwerker kan en mag dus zelfstandig alleen iets met de gegevens die hij voor Groeisaam verwerkt indien dat conform de instructies en richtlijnen van de verantwoordelijke plaatsvindt. Groeisaam bepaalt het doel en de middelen. Zo is de salarisadministrateur een verwerker als ook het softwarebedrijf dat de hosting doet en/of de applicatie beschikbaar stelt en/of het onderhoud doet.
Net zoals Groeisaam verantwoordelijk is voor adequate beveiliging van de persoonsgegevens op organisatorisch en technisch niveau, geldt dit evenzeer voor de verwerker.
In veel gevallen is de verwerker de eerste die kennis heeft van een datalek. Groeisaam is echter verantwoordelijk voor het (laten) melden van dit lek, dat bij de verwerker is ontstaan. Het is daarom van belang dat de verwerker het lek direct meldt aan Groeisaam.
Met deze verwerkers heeft Groeisaam afspraken gemaakt in de verwerkersovereenkomst voor het melden van een datalek. Van deze verwerkers is in kaart gebracht welke gegevens worden verwerkt en voor welke doeleinden. Dit is geregistreerd in het verwerkingsregister van Groeisaam.

6 Hoe moet een datalek gemeld worden?

6.1 Melding aan de AP

Een datalek moet **onverwijld** (*onverwijld: zonder onnodige vertraging, en niet later dan 72 uur na de ontdekking van het datalek*) gemeld worden aan de Autoriteit Persoonsgegevens.
De termijn voor het melden begint te lopen op het moment dat Groeisaam of de verwerker op de hoogte raakt van een incident waarbij persoonsgegevens kunnen zijn blootgesteld aan verlies of onrechtmatige verwerking.
Voor het feitelijk doen van de melding stelt de AP een **webformulier** beschikbaar[3]. In de melding moet worden aangegeven of het datalek ook aan betrokkene is gemeld.
Uiteraard dient, nadat het datalek is geconstateerd, direct te worden overgegaan tot het treffen van corrigerende acties in overleg met een privacydeskundige en/of informatiebeveiligingskundige.

6.2 Melding aan de FG

Een datalek wordt direct gemeld aan de Functionaris Gegevensbescherming. In overleg met de Functionaris Gegevensbescherming zal besproken worden welke acties er verder moeten worden ondernomen.

6.3 Melding aan betrokkene.

Naast het melden aan de Autoriteit Persoonsgegevens moet het datalek in de meeste gevallen ook gemeld worden aan (alle) betrokkene(n). Zie voor verdere details paragraaf 8.3.4.

7 Registratie bijhouden van beveiligingsincidenten c.q. datalekken

Groeisaam houdt een register bij van alle beveiligingsincidenten en van datalekken die onder de meldplicht vallen. Het register valt onder de verantwoordelijkheid van de privacycoördinator van Groeisaam. Per datalek worden bijgehouden de feiten en gegevens omtrent de aard van de inbreuk. Tevens wordt de tekst van de melding aan betrokkenen opgenomen. Dit register wordt minimaal één jaar bewaard. Tevens is het goed steeds de getroffen maatregelen te vermelden die zijn toegepast om de risico's en consequenties van het incident (direct en naar de toekomst toe) te beperken. Dit register is niet openbaar.

8 Interne procedure

8.1 Constateren van een mogelijk datalek door medewerker en interne melding

Indien een medewerker van Groeisaam een mogelijk datalek signaleert, is deze verplicht deze onverwijld intern te melden. De melding kan gedaan worden via de homepagina van de Intranetsite van Groeisaam.
Hierbij handelt de medewerker als volgt:

1. Het direct na ontdekking opstellen van een mailbericht aan de leidinggevende en aan de privacycoördinator, zijnde het **Quick Response Team**, met daarin een omschrijving van de volgende gegevens:
   - Wat is er precies gebeurd: een duidelijke omschrijving van het incident.
   - Is het incident zelf ontdekt (intern) of via een externe bron (verwerker, of andere derde).
   - Tijdstip (datum en tijd) van het datalek.
   - Welke persoonsgegevens zijn hierbij betrokken.
2. Verzamel zo veel mogelijk bewijs en bewaar dit zorgvuldig.

3 Zie: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0.

Na ontvangst van de melding neemt de privacycoördinator de melding op in het meldingsregister en stelt hij het stappenplan datalekken in werking (bijlage 3).

8.2 Quick Response Team

De privacycoördinator en het bovenschools ICT team vormen het **Quick Response Team** van Groeisaam. Het **Quick Response Team** maakt afspraken over aanwezigheid en vervanging. Het **Quick Response Team** houdt bij het beoordelen van mogelijke datalekken rekening met de stappen in dit document en onderzoekt het beveiligingsincident.

Na een ontvangen melding worden de volgende stappen ondernomen:

8.2.1 Afweging datalek

- Binnen 2 uur na de melding: start met het beoordelen van de interne melding in samenspraak met de Functionaris Gegevensbescherming.

Doel: uitzoeken of er sprake is van een ***mogelijk*** beveiligingsincident en ***mogelijk*** datalek.

- Zo ja: melden van het mogelijke datalek aan de bestuurder.
- Dossier aanmaken (*jaartal en nummer/tijdstip/naam melding*).
- Register Beveiligingsincidenten/Datalekken[4] bijwerken: dossiernummer toevoegen.
- Afweging maken of er sprake is van een datalek.
- Afweging maken of er een melding van een incident aan de AP moet worden gedaan.

In geval dat het incident niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens is er geen sprake van een datalek maar van een beveiligingslek. Melding aan de AP is dan niet aan de orde. Wel kan in het overleg besloten worden, dat het zinvol is om het beveiligingslek te onderzoeken om herhaling te voorkomen.

- Is dit niet het geval: dossier sluiten met duidelijke motivering en conclusie en register bijwerken.
- Is dit wel het geval: Quick Response Team meldt aan de bestuurder.

8.2.2 Direct te treffen maatregelen

Welke maatregelen moeten worden getroffen? Dit is afhankelijk van de aard, ernst en omvang van het datalek.

Het **Quick Response Team** neemt hierbij de volgende overwegingen mee:

- Bewijs veilig stellen.
- Is er sprake van een kwetsbaarheid in de beveiliging van systemen?
- Is er sprake van betrokkenheid van een verwerker?
- Kan schade beperkt worden? Denk hierbij aan IT oplossingen om bestanden veilig te stellen, maatregelen om toegang te voorkomen.
- Zijn bijzondere gegevens gelekt: medische gegevens, BSN, financiële gegevens?
- Zijn belangen van betrokkenen geschaad (*ernstige nadelige gevolgen of risico voor de rechten en vrijheden van natuurlijke personen: is er sprake van een omvangrijke groep van personen, of bijzondere gegevens*)?
- Welke internen moeten worden betrokken? Denk hierbij aan de verantwoordelijke managers en medewerkers waar zich het incident heeft voorgedaan.
- Moeten externen worden ingeschakeld? Denk aan deskundigen op het gebied van privacy en ICT.
- Moet er rekening gehouden worden met publiciteit? Denk aan pers/media aandacht.

4 Dit register moet minimaal één jaar worden bewaard.

- Moet de politie worden ingeschakeld? Dit is aan de orde indien er sprake is van een strafbaar feit (bijvoorbeeld hacking: art. 138ab Wetboek van Strafrecht[5]).

8.3 Meldplicht

8.3.1 Melding aan Autoriteit Persoonsgegevens

Indien er sprake is van een datalek, dan moet er tijdig (*onverwijld, zonder onnodige vertraging, en niet later dan 72 uur na de ontdekking van het beveiligingsincident*) een digitale melding bij de Autoriteit Persoonsgegevens worden gedaan volgens het online meldingsformulier[6]. Dit met inachtneming van richtlijnen van de AP terzake.
De verantwoordelijke vult het formulier in en doet de melding aan de Autoriteit Persoonsgegevens. Vóórdat het formulier wordt verzonden vindt er afstemming plaats met de bestuurder. De bestuurder van Groeisaam is formeel 'de melder'. De verantwoordelijke is de gedelegeerde 'contactpersoon' voor de communicatie tussen Groeisaam en de Autoriteit Persoonsgegevens. Dit geldt ook ingeval nog niet duidelijk is dat het incident een datalek is. Dan is de mogelijkheid aanwezig om na vaststelling van de aard van het incident de melding aan te vullen dan wel in te trekken.
Nadat het formulier aan de Autoriteit Persoonsgegevens is verzonden, moet Groeisaam zelf een kopie van de melding downloaden. Groeisaam ontvangt direct een ontvangstbevestiging, welke in het dossier en in het Register Datalekken wordt toegevoegd.

8.3.2 Melding aan betrokkene

De afwegingen, of datalekken aan betrokkene(n) gemeld moeten worden, zijn:

- Bieden de technische en organisatorische beschermingsmaatregelen die zijn genomen voldoende bescherming om de melding aan betrokkene achterwege te kunnen laten? *Dit geldt bijvoorbeeld indien het vanwege technische beveiliging (encryptie) absoluut is uitgesloten dat iemand bij de persoonsgegevens kan komen.*
- Houdt het datalek een hoog risico in voor de rechten en vrijheden (waarschijnlijk ongunstige gevolgen) van betrokkene*? Indien het gaat om medische gegevens, financiële gegevens, BSN, kopie legitimatiebewijs, wordt aangenomen dat dit meestal het geval is.*

In het bericht aan de betrokkene wordt gemeld:

- De aard van de inbreuk.
- De contactpersoon waar de betrokkene meer informatie kan krijgen over de inbreuk.
- De maatregelen die worden aanbevolen te nemen om de negatieve gevolgen van de inbreuk te beperken (bijvoorbeeld het wijzigen van het wachtwoord of veiligstellen van gegevens).

De mededeling moet eveneens onverwijld plaatsvinden.
Bij twijfel of een incident/datalek gemeld moet worden aan betrokkene of toezichthouder is het raadzaam om contact op te nemen met de Autoriteit Persoonsgegevens.

- De melder van het datalek wordt op de hoogte gehouden/ gebracht van het doorlopen proces.

8.3.3 Leren van datalekken

Op basis van de gegevens die betrekking hebben op het datalek wordt door het Quick Response Team een analyse gemaakt. Hierbij komen oorzaak, gevolgen en mitigerende maatregelen aan de orde. Tevens wordt aangegeven welke lessen uit het incident naar voren komen en hoe soortgelijke

5 Computervredebreuk. Hierop staat een gevangenisstraf van twee of vier jaar (indien de gegevens ook nog onrechtmatig worden gebruikt), of een geldboete van de vierde categorie.

6 Zie: https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?1

datalekken naar de toekomst toe voorkomen kunnen worden. Deze analyse wordt aan het dossier toegevoegd.
Het dossier en de analyse worden besproken in het overleg met de bestuurder.

Bijlage 1

Artikel 33 AVG

Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit

1. Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.
2. De verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.
3. In de in lid 1 bedoelde melding wordt ten minste het volgende omschreven of meegedeeld:
   a. de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
   b. de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
   c. de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
   d. de maatregelen die de verwerkingsverantwoordelijke 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 nadelige gevolgen daarvan.
4. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.
5. De verwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren.

Artikel 34 AVG

Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene

1. Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.
2. De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in artikel 33, lid 3, onder b), c) en d), bedoelde gegevens en maatregelen.
3. De in lid 1 bedoelde mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:
   a. de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
   b. de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het in lid 1 bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;

c. de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

4. Indien de verwerkingsverantwoordelijke de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de toezichthoudende autoriteit, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, de verwerkingsverantwoordelijke daartoe verplichten of besluiten dat aan een van de in lid 3 bedoelde voorwaarden is voldaan.

Bijlage 2

In deze bijlage is de interne procedure opgenomen, welke geldt voor iedere medewerker van Groeisaam om een datalek te melden.

Binnen Groeisaam werken we veel met persoonlijke en dus vertrouwelijke gegevens. Denk hierbij bijvoorbeeld aan medische gegevens, e-mail adressen, inloggegevens en wachtwoorden. Al deze informatie is terug te leiden tot een persoon. Hier moeten wij als organisatie zorgvuldig mee omgaan, dat spreekt voor zich.
Een verloren USB-stick met informatie over leerlingen die niet encrypted is? Een dossier voor advies in de trein laten liggen? E-mail van Groeisaam met leerlinggegevens gestolen? Je computer is gehackt? Je hebt een mail met persoonsgegevens per ongeluk naar een verkeerd mailadres gestuurd? Dit zijn allemaal voorbeelden van mogelijke datalekken; persoonsgegevens zijn verloren gegaan, liggen 'op straat' of zijn niet meer toegankelijk. Groeisaam is verplicht deze datalekken te melden bij de Autoriteit Persoonsgegevens. Daarbij wordt dan tevens bepaald welke vervolgstappen nodig zijn en welke maatregelen genomen moeten worden om te voorkomen dat dit nogmaals gebeurt.

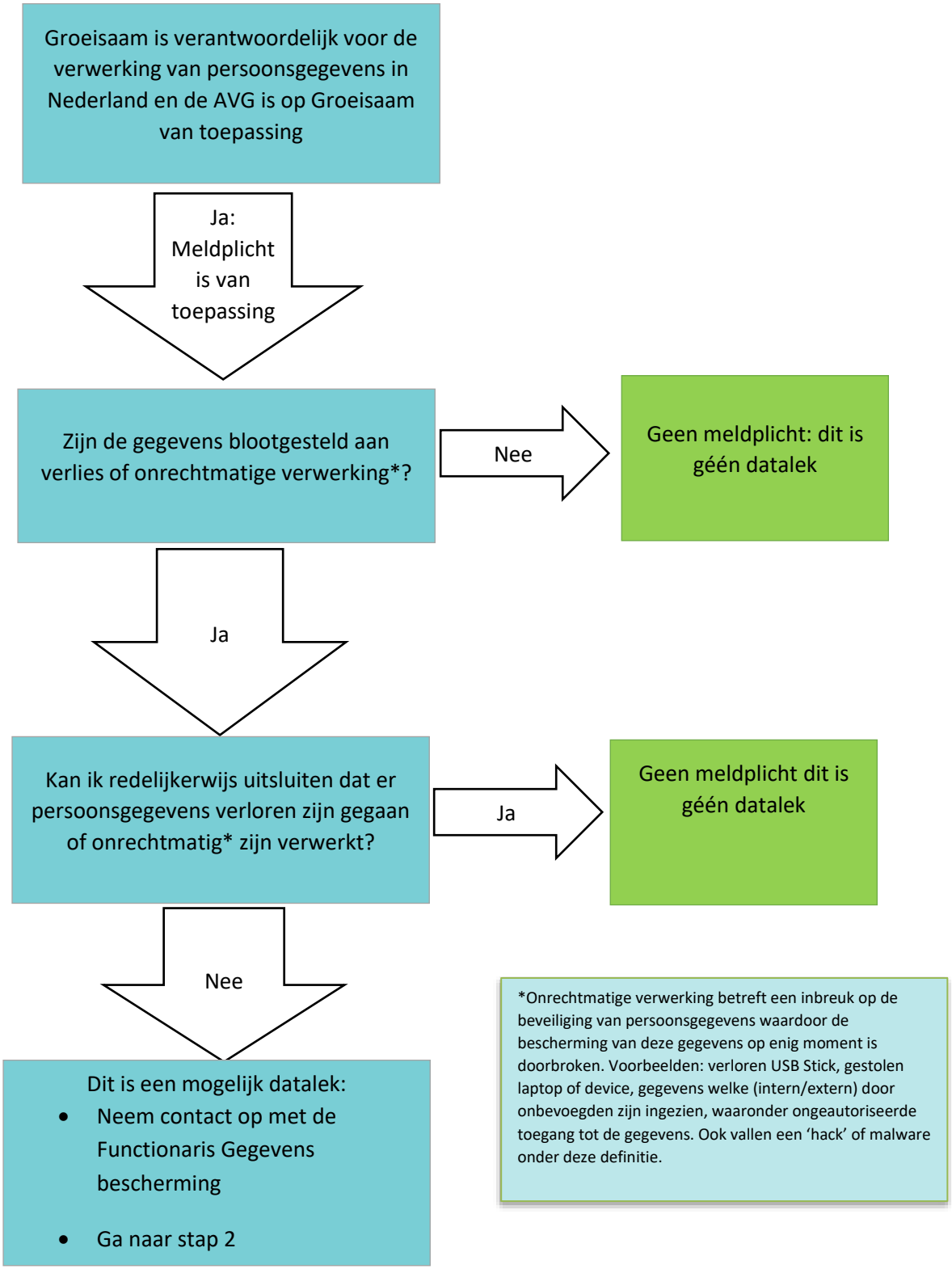
Indien een medewerker van Groeisaam een mogelijk datalek signaleert, is deze verplicht deze onverwijld te melden.

Hierbij handelt de medewerker als volgt:

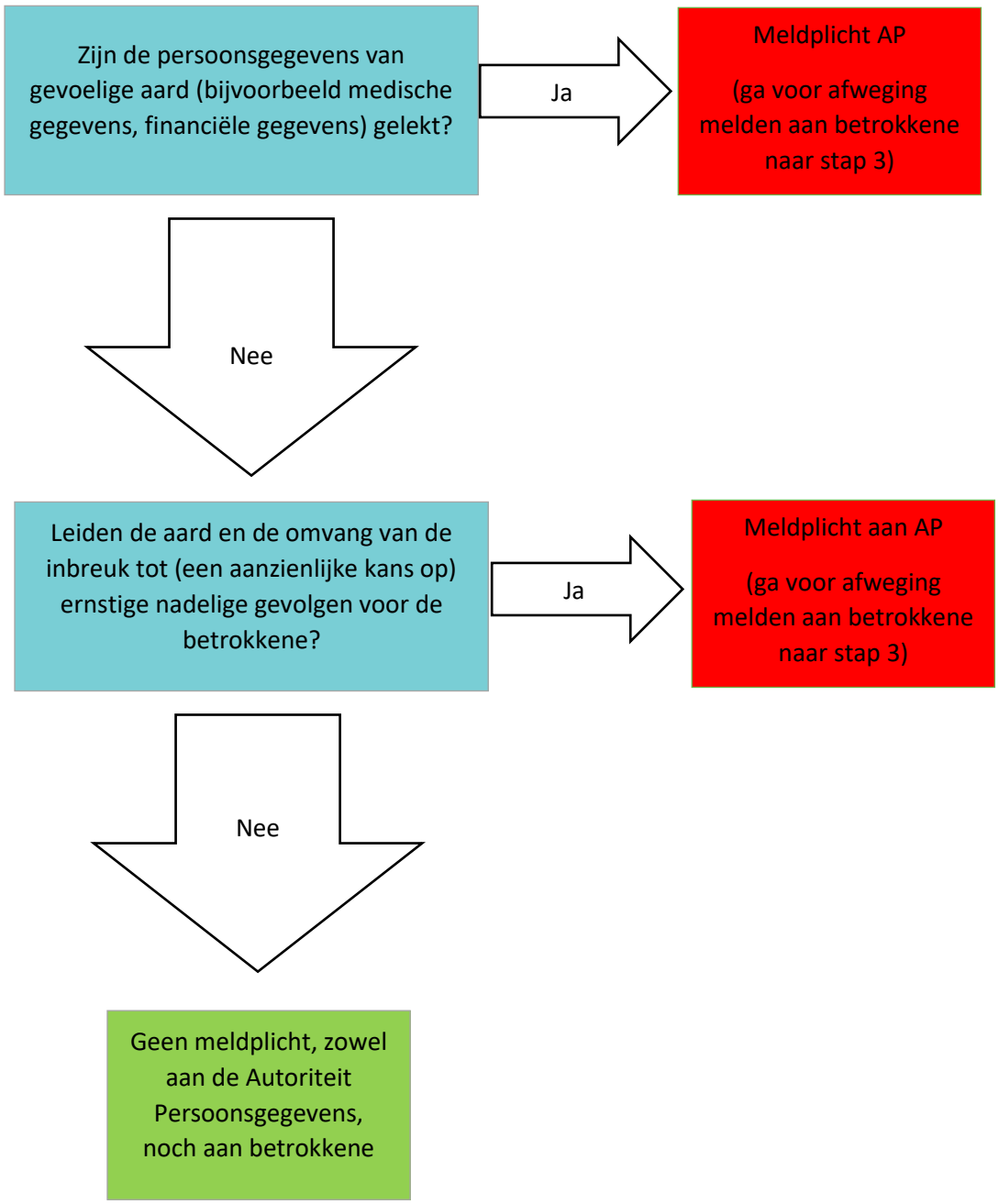
1. De medewerker doet direct na ontdekking van een incident melding hiervan aan de privacycoördinator/het **Quick Respons Team** via de homepage van de Intranetsite van Groeisaam, dan wel via een mail naar datalek@groeisaampo.nl met daarin een omschrijving van de volgende gegevens:
    - Wat er precies gebeurd is: een zo duidelijk mogelijke omschrijving van het incident.
    - Is het incident zelf ontdekt (intern) of via een externe bron (verwerker, of andere derde).
    - Tijdstip van het incident (datum en tijd).
    - Welke persoonsgegevens zijn hierbij betrokken.
2. De privacycoördinator zorgt voor melding van het incident in het register van beveiligingsincidenten.
3. Verzamel zo veel mogelijk bewijs en bewaar dit zorgvuldig.

Bijlage 3

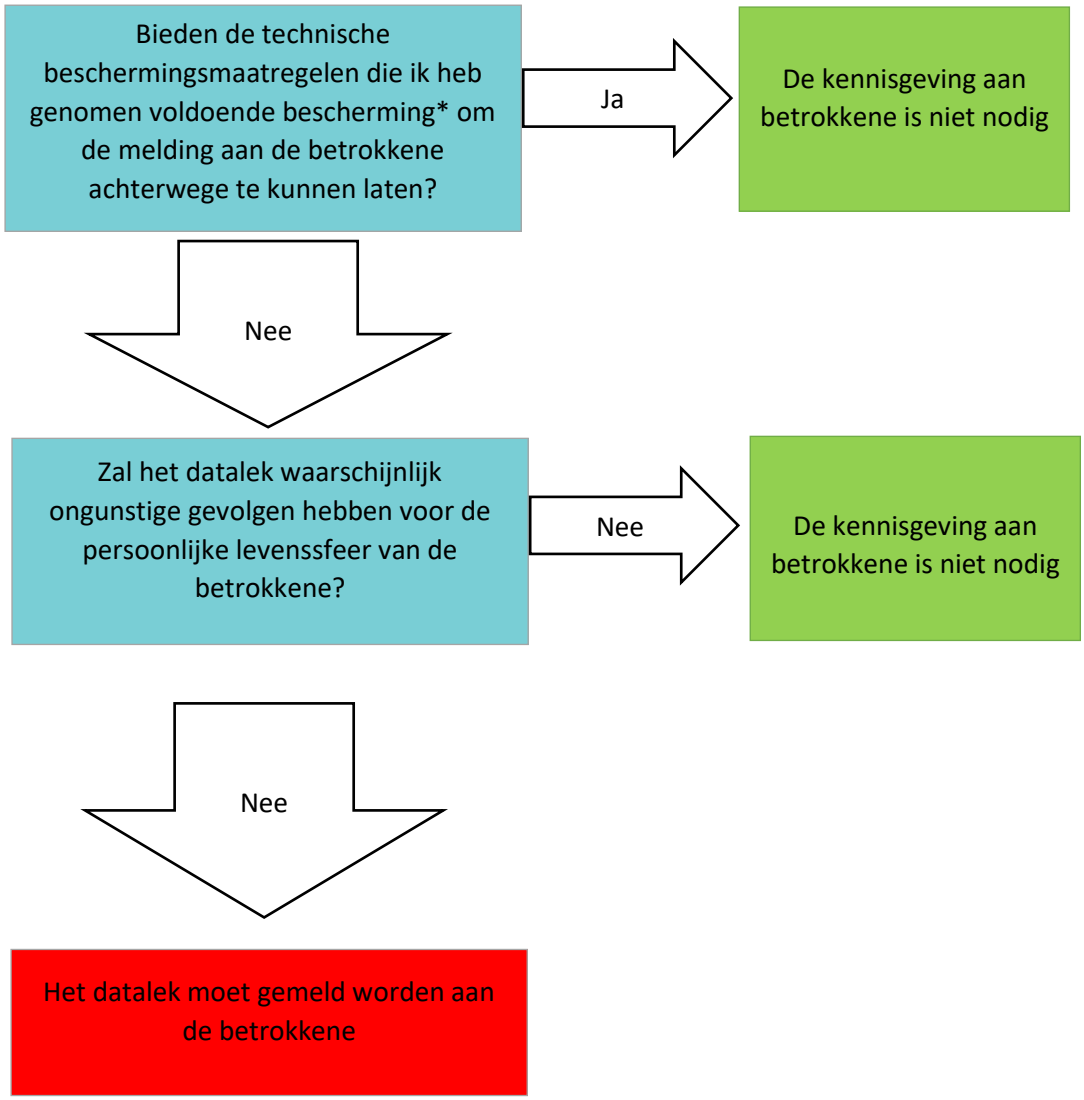
Stappenplan Datalekken/Stap 1: Is het datalek meldingsplichtig richting Autoriteit Persoonsgegevens ?



Stappenplan Datalekken/Stap 2: Is het waarschijnlijk dat de inbreuk een risico inhoudt voor de rechten en vrijheden van betrokkenen: is er sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens?



Stappenplan Datalekken/Stap 3: Moet ik het datalek melden aan betrokkene?



*Het betreft hier bijvoorbeeld beveiligingsmaatregelen zoals encryptie van een laptop, zodanig dat de persoonsgegevens niet te lezen zijn door onbevoegden.