AVG

Protocol Datalekkenbeleid

Wat te doen bij een datalek?

optimus

Inhoud

1 Inleiding

In dit protocol wordt de meldplicht die Stichting Optimus Primair Onderwijs heeft in het kader van artikel 33 en 34 AVG uitgewerkt. Stichting Optimus is in de zin van de AVG 'verwerkingsverantwoordelijke' voor de verwerking van persoonsgegevens. Stichting Optimus is daarom verplicht datalekken direct 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 Stichting Optimus omgaat met datalekken en wanneer een datalek vanuit Stichting Optimus 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 Stichting Optimus . Voor verwerkers geldt dat indien zij geconfronteerd worden met een datalek, zij dit onverwijld aan de privacy-coördinator van Stichting Optimus moeten doorgeven, zodat deze namens Stichting Optimus 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 Stichting Optimus gaat het om leerlinggegevens, gegevens van ouders/verzorgers en gegevens van medewerkers.
Stichting Optimus 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 Informatie Privacy Beleid (IBP-beleid) van Stichting Optimus 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.

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

1.1 Definities

De volgende definities worden gehanteerd:

AP	Autoriteit Persoonsgegevens.
AVG	General Data Protection Regulation, welke verordening geldt per 25 mei 2018.
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.
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 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. Stichting Optimus (artikel 4 sub 10 AVG).
Easy Privacy	Programma voor bovenschools IBP beleid Optimus PrivacyTeam
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).
IBP	Informatie en privacy beleid.
IBP-team	Dit is het interne team binnen Stichting Optimus om een incident te onderzoeken alsmede hieraan opvolging te geven. Het IBP-team heeft de regie over het afhandelen van het incident, en zorgt voor nakoming van alle wettelijke verplichtingen. Het IBP-team bestaat uit het bestuur, de privacy-coördinator, de coördinator ICT en de communicatieadviseur. Zie bijlage 4.
Persoonsgegeven	Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4 sub 1 AVG).

Phishing	Phishing is een vorm van internetfraude. Het bestaat uit het oplichten van mensen door ze te lokken naar valse websites om persoonlijke en gevoelige gegevens ‘binnen te hengelen’. Het aas is vaak een nep e-mail waarmee ze zich voordoen als je bank, overheidsinstelling, postbedrijf, webwinkel, maar dus ook een bedrijf dat software levert aan jouw school. Via de e-mail doen ze je het verzoek om op linkjes te klikken, bijlages te openen, geld over te maken of gegevens in te vullen. Op die manier kunnen ze zorgen voor de verspreiding van virussen, persoonsgegevens buitmaken of geldsommen aftroggelen.
Privacy-coördinator	Medewerker op sturend niveau voor wat betreft de AVG. Deze medewerkers is inhoudelijk verantwoordelijk voor IBP, voor de IBP- planning en controle en adviseur voor het CvB.
Ransomware	Ransomware of gijzelsoftware is een computervirus dat als doel heeft om je geld te laten betalen om van het virus af te komen. Ransomware kaapt je computer door bijvoorbeeld bestanden te blokkeren waardoor ze niet meer toegankelijk zijn. Pas als je losgeld (ransom) betaalt zou je de computer of de bestanden weer kunnen gebruiken.
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: Stichting Optimus .
Verwerker	Degene die ten behoeve van Stichting Optimus (als verwerkingsverantwoordelijke) persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen (artikel 4 sub 8 AVG: ‘verwerker’).
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).

2 Wanneer is er sprake van een datalek?

Bij een datalek gaat het om toegang tot of vernietiging van, verloren gaan van, wijziging of vrijkomen van persoonsgegevens bij Stichting Optimus zonder dat dit de bedoeling is van Stichting Optimus of de scholen die onder Stichting Optimus vallen. Let op: er wordt onderscheid gemaakt tussen een beveiligingsincident en een datalek, zoals bedoeld in de AVG. Bij een beveiligingsincident is er *mogelijk* sprake van schade of misbruik van persoonsgegevens. Bij een datalek is dit een zekerheid.

Datalek melden
Alle beveiligingsincidenten en datalekken worden gemeld via privacycoordinator@optimusonderwijs.nl.

Bij een datalek nemen we altijd contact op met de Functionaris Gegevensbescherming om het datalek te bespreken.

Voorbeelden van een datalek zijn:

- een USB-stick is kwijt geraakt[2];
- de mobiele telefoon is verloren of gestolen, die ook voor het werk gebruikt wordt met daarin telefoonnummers van collega's of informatie van leerlingen/ouders;
- een email met persoonsgegevens, bijvoorbeeld een rapport over een leerling wordt naar een verkeerd email adres gestuurd;
- een leerling heeft het schoolnetwerk gehackt en kan bij de wachtwoorden;
- door een fout in het toekennen of intrekken van toegangsrechten bijvoorbeeld bij ParnasSys hebben onbevoegden toegang tot deze gegevens;
- een collega heeft een phishing mail geopend waardoor er malware is geïnstalleerd die toegang tot persoonsgegevens tot gevolg heeft;
- 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;
- een malware besmetting;
- een calamiteit, zoals een brand in een datacentrum.
- Ook fysieke documenten vallen onder het begrip datalek. Dit betekent wanneer in openbare ruimtes maar ook klaslokalen, bureaus, printers e.d. persoonlijke gegevens niet afgeschermd zijn en door onbevoegden ingezien hadden kunnen worden is dit een beveligingsincident/datalek. Denk hierbij aan openstaande kasten met gevoelige gegevens.
- Ook aanmeldformulier en/of inschrijfformulier van leerlingen moeten zo worden bewaard, dat alleen personen met toegangsrecht toegang hebben tot deze formulieren. Indien anderen toegang zouden kunnen hebben, is dit ook een beveiligingsincident of datalek en zal gemeld moeten worden.

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

[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 zwaarbeveiligd 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'.

beveiligingsincident is alleen een datalek als wordt voldaan aan de voorwaarden zoals gesteld in hoofdstuk 4.

3 Wat is er precies aan de hand bij 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.

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?

In alle gevallen wordt een datalek gemeld bij de privacy-coördinator van Stichting Optimus. Alle meldingen worden vermeld door de prinvacy-coördinator in het incidentenregister.

Er zijn vervolgens twee mogelijkheden of deze datalek gemeld moet worden bij de Autoriteit Persoonsgegevens:

1. 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.
2. 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. Dit wordt gedaan door de privacy-coördinator in samenwerking met de Functionaris Gegevensbescherming en het College van Bestuur.

Hiervan is sprake in de volgende gevallen:

- indien er persoonsgegevens van gevoelige aard gelekt zijn (*Indien 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.

5 Bepalingen voor de verwerker

Voor verwerkers geldt dat indien zij geconfronteerd worden met een datalek, dit onverwijld aan de privacy-coördinator van Stichting Optimus moeten doorgeven, zodat deze namens Stichting Optimus de melding kan doen. De afwegingen voor melding worden in samenspraak besloten door de privacy-coördinator, de Functionaris Gegevensbescherming en het CvB.

Een verwerker verwerkt persoonsgegevens ten behoeve van de verantwoordelijke (i.c. Stichting Optimus), enkel en alleen op instructie van de verantwoordelijke. De verwerker kan en mag dus zelfstandig niets met de gegevens die hij voor Stichting Optimus verwerkt. Stichting Optimus 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 Stichting Optimus 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. Stichting Optimus 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 Stichting Optimus .
Met deze verwerkers heeft Stichting Optimus afspraken gemaakt in de verwerkersovereenkomst voor het melden van een datalek.

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 Stichting Optimus of de verwerker op de hoogte raakt van een incident waarbij persoonsgegevens kunnen zijn blootgesteld aan verlies of onrechtmatige verwerking. Stichting Optimus roept dan het IBP-team bij elkaar en brengt de Functionaris Gegevensbescherming op de hoogte.

Voor het feitelijk doen van de melding stelt de AP een **webformulier** beschikbaar[3]. In de melding moet worden aangegeven of de 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 privacy deskundige en/of informatiebeveiligingskundige.

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

6.2 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. Dit gebeurt altijd door de privacy-coördinator en het CvB.

7 Registratie bijhouden van beveiligingsincidenten c.q. datalekken

Stichting Optimus houdt een register bij van alle beveiligingsincidenten en van datalekken die onder de meldplicht vallen. Het register valt onder de verantwoordelijkheid van de privacy coördinator van Stichting Optimus. 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 Stichting Optimus een mogelijk datalek signaleert, is deze verplicht deze onverwijld intern te melden bij de privacy-coördinator: privacycoordinator@optimusonderwijs.nl.

De instructie voor medewerkers is te vinden op WOOW, het intranet van Stichting Optimus. De instructie is opgenomen als **bijlage 2**. De infographic hangt zichtbaar in iedere personeelskamer.

Hierbij handelt de medewerker als volgt:

1. Het direct na ontdekking opstellen van een mailbericht aan de leidinggevende en aan de privacy coördinator, zijnde het **IBP-team** met daarin een omschrijving van de volgende gegevens:
    - Wat is er precies gebeurd? : zo duidelijk mogelijke omschrijving van het incident.
    - Is het incident zelf ontdekt (intern) of via een externe bron (verwerker, of andere derde)?
    - Welk tijdstip (datum en tijd)?
    - Welke persoonsgegevens zijn hierbij betrokken.
2. Verzamel zo veel mogelijk bewijs en bewaar dit zorgvuldig.
3. Vermeld het brinnummer en de betrokken personen.

8.2 IBP-team

Het CvB, de privacy coördinator, de Functionaris Gegevensbescherming en de communicatieadviseur, en indien nodig de ICT-coördinator vormen het **IBP-team** van Stichting Optimus Onderwijs.

Het **IBP-team** maakt afspraken over aanwezigheid en vervanging. Het **IBP-team** houdt bij het beoordelen van mogelijke datalekken rekening met de stappen in dit document en onderzoekt het beveiligingsincident.

Na een ontvangen melding via privacycoordinator@optimusonderwijs.nl worden de volgende stappen beschreven in paragraaf 8.3 ondernomen.

8.3 Afweging datalek door IBP-team

Volg de stappen in bijlage 3

- Binnen 2 uur na de melding: starten met het beoordelen van de interne melding.
  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*) in Easy Privacy door de privacy-coördinator
- Register Beveiligingsincidenten / Datalekken bijwerken: dossiernummer toevoegen in Easy Privacy.
- Afweging maken of er sprake is van een datalek.
- Afweging maken of er een melding van een incident aan de AP moet worden gedaan. de melding aan de AP wordt altijd vooraf gegaan door een overleg van het **IBP-team** en de Functionaris Gegevensbescherming.

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.

- Zo neen: dossier sluiten met duidelijke motivering en conclusie en register bijwerken in Easy Privacy.
- Zo ja**: privacy-coördinator** meldt vervolgstappen aan het College van Bestuur.

8.4 Direct te treffen maatregelen

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

Het **IBP-team** neemt hierbij de volgende overwegingen mee:

- Bewijs veiligstellen.
- 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.
- 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[4]).

9 Meldplicht

9.1 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[5]. Dit met inachtneming van richtlijnen van de AP terzake.

Het IBP-team vult samen met de schoolleider en de medewerker het formulier in, stemt af met de FG en doet daarna pas melding aan de Autoriteit Persoonsgegevens. Het College van Bestuur van Stichting Optimus is formeel ‘de melder’. De verantwoordelijke is de privacy-coördinator voor de communicatie tussen Stichting Optimus 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, ontvangt Stichting Optimus direct een ontvangstbevestiging, welke in het dossier op Easy Privacy en in het Register Datalekken wordt toegevoegd.

9.2 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.*

[4] 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.
[5] Zie: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

- Zijn er zwaarwegende redenen om de melding aan betrokkene achterweg te laten? (*Kan de melding aanleiding geven tot risico's voor de samenleving, zoals vermindering van vertrouwen van het publiek of de relevante markt.)*.

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, en 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 zowel de Autoriteit Persoonsgegevens.

9.3 Leren van datalekken

Op basis van de gegevens die betrekking hebben op het datalek, wordt door het IBP-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 datalekken naar de toekomst toe voorkomen kunnen worden. Deze analyse wordt aan het dossier toegevoegd.

Het dossier en de analyse wordt besproken in het overleg met het College van Bestuur en besproken in het directeurenoverleg van Stichting Optimus .

Bijlage 1 artikelen 33 en 34 AVG

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 vergezelt 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 Interne procedure melden datalek

VOLG DE INFOGRAPHIC IN DE LERARENKAMER
In deze bijlage is de interne procedure opgenomen, welke geldt voor iedere medewerker van Stichting Optimus Om een datalek te melden.

Binnen Stichting Optimus werken we veel met persoonlijke en dus vertrouwelijke gegevens. Denk hierbij bijvoorbeeld aan leerling gegevens, medische gegevens, e-mailadressen, inloggegevens en wachtwoorden. Al deze informatie is terug te leiden tot een persoon. Hier moeten wij als organisatie natuurlijk zorgvuldig mee omgaan, dat spreekt voor zich.

Een verloren laptop met informatie over leerlingen die niet encrypted is? Een dossier voor advies in de trein laten liggen? E-mail van Stichting Optimus met leerling gegevens 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. Stichting Optimus is verplicht deze datalekken te melden bij de Autoriteit Persoonsgegevens. Daarbij wordt dan tevens bepaald welke vervolgstappen nodig zijn en aan maatregelen die genomen moeten worden om te voorkomen dat dit nogmaals gebeurt.

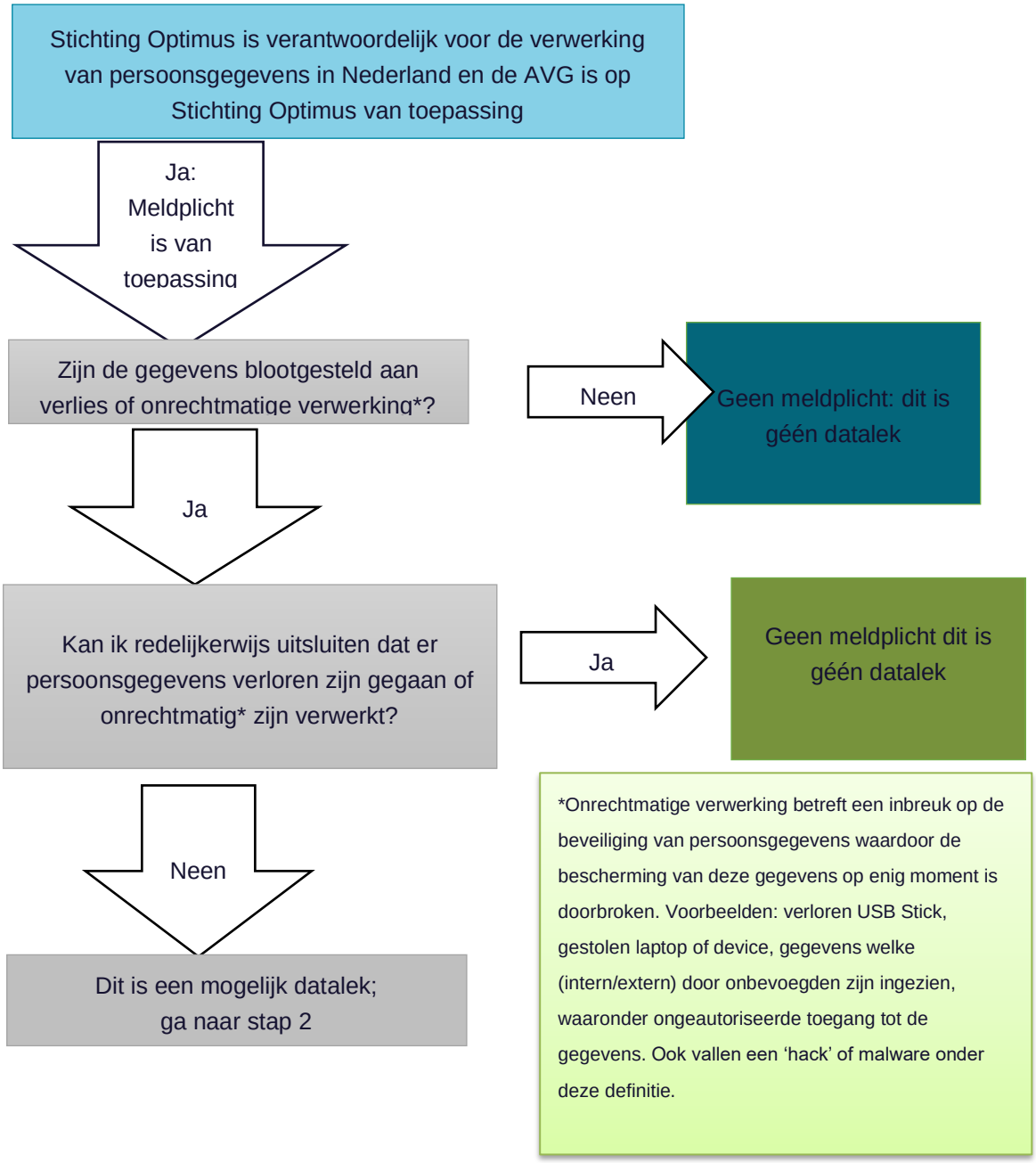
Indien een medewerker van Stichting Optimus een mogelijk datalek signaleert, is deze verplicht deze DIRECT te melden bij de privacy-coördinator: privacycoördinator@optimusonderwijs.nl

Hierbij handelt de medewerker als volgt:

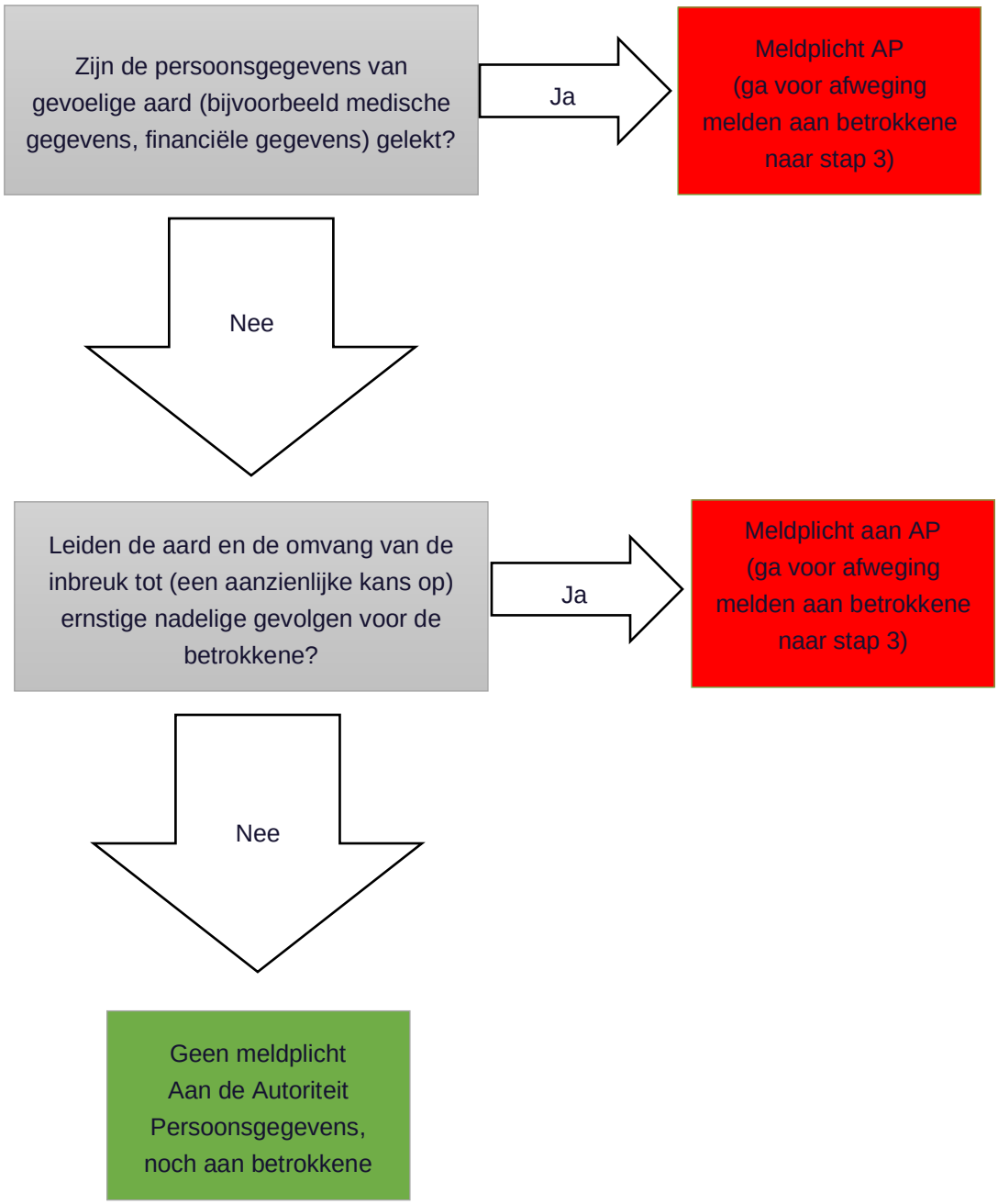
1. Het direct na ontdekking van een incident melding hiervan doen aan de leidinggevende en het IBP-team, met daarin een omschrijving van de volgende gegevens:
    a. Wat is er precies gebeurd: zo duidelijk mogelijke omschrijving van het incident?
    b. Is het incident zelf ontdekt (intern) of via een externe bron (verwerker, of andere derde)?
    c. Welk tijdstip (datum en tijd)?
    d. Welke persoonsgegevens zijn hierbij betrokken?
2. Volg het uitgebreide stappenplan uit bijlage 3 om vast te stellen of het een incident of een datalek is. Bij twijfel altijd de privacy-coördinator inschakelen.
3. Mail alle gegevens naar: privacycoordinator@optimusonderwijs.nl.
4. De privacy-coördinator zorgt voor opname in het register van beveiligingsincidenten en in Easy Privacy en verdere verwerking en schakelt eventueel het IPB-team in voor de te nemen stappen.
5. Verzamel zo veel mogelijk bewijs en bewaar dit zorgvuldig.

Bijlage 3 Stappenplan Datalekken /

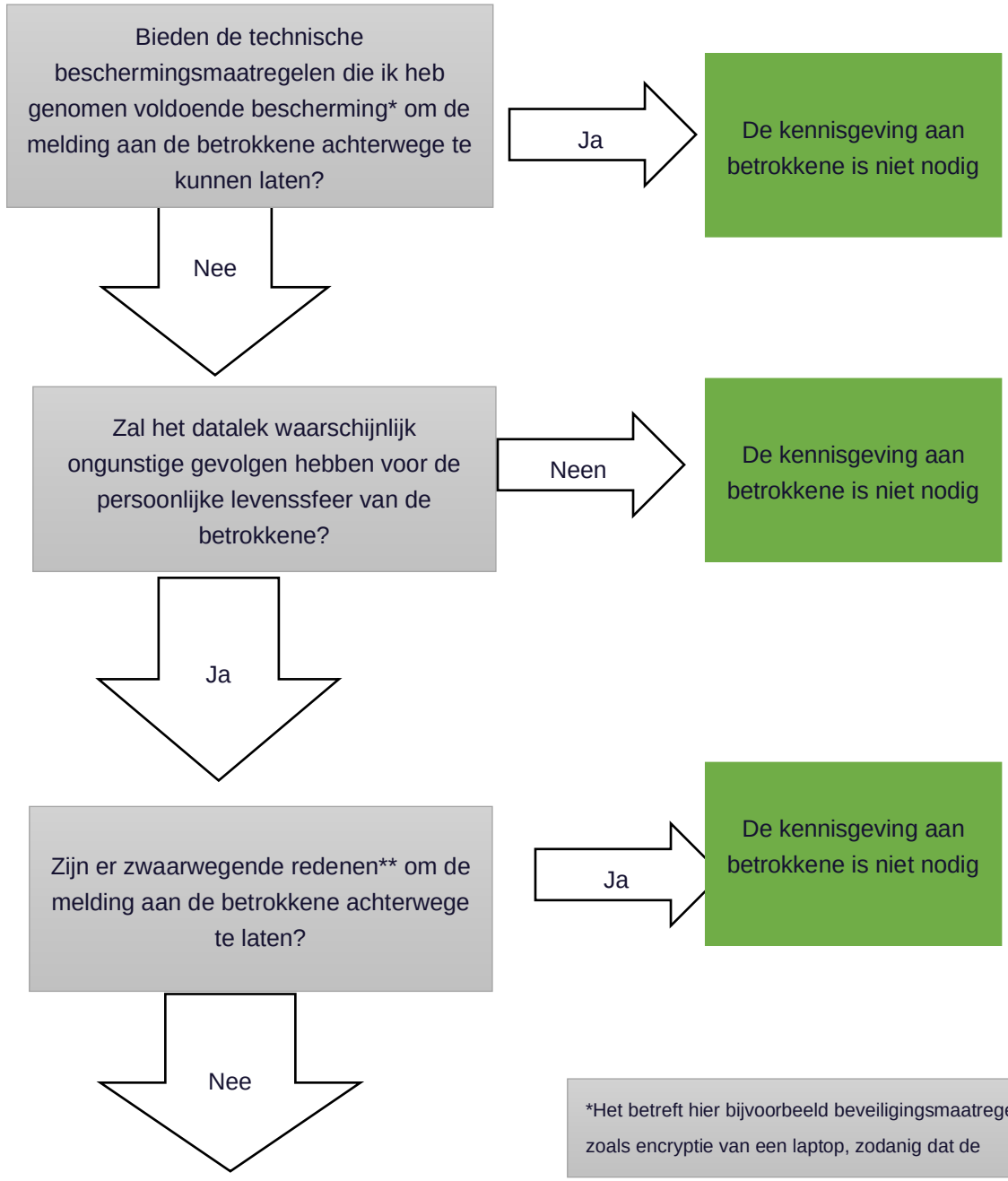
Stap 1: Is de datalek meldingsplichtig richting Autoriteit Persoonsgegevens ?



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?



Stap 3: Moet ik de datalek melden aan betrokkene?



*Het betreft hier bijvoorbeeld beveiligingsmaatregelen zoals encryptie van een laptop, zodanig dat de

**Bij zwaarwegende redenen moet u denken aan de situatie dat het achterwege laten van de melding noodzakelijk is met het oog op de belangen van de betrokkene en/of de staat: veiligheid van de staat, voorkoming, opsporing en vervolging van strafbare feiten, gewichtige economische en financiële belangen van de staat en de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

Bijlage 4 Taken bevoegdheden en verantwoordelijkheden IBP team

Eindverantwoordelijke
Het College van Bestuur is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.
De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd.
De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de privacy coördinator.

Opdracht IBP-team
Het IBP-team van Stichting Optimus primair onderwijs heeft de volgende opdracht:

- Het signaleren en registreren van alle privacy verzoeken, beveiligingsincidenten en datalekken. Het coördineren van de maatregelen en het toezien op de oplossing van problemen die tot incidenten hebben geleid of waardoor de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij);
- Het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheerders, ontwikkelaars en eindgebruikers door het verspreiden van informatie;
- Het leveren van managementrapportages en verbetervoorstellen aan de domeinverantwoordelijke/proceseigenaren over de beveiligingsincidenten en verzoeken tot uitoefening privacy rechten van de betrokkenen.

Bij een calamiteit kan het IBP-team terstond bij elkaar worden geroepen op initiatief van de privacy coördinator, in opdracht van het Stichting Optimus Onderwijs Het doel hiervan is om de **continuïteit** van de informatievoorziening en de privacy te waarborgen. Onder calamiteiten worden verstaan:

- Datalek;
- Grote verstoringen van het netwerk (bijvoorbeeld DDoS aanval);
- Natuurrampen (brand, overstroming, storm, etc.).

Het IBP-team bij Stichting Optimus Onderwijs behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident.
De werkzaamheden van het IBP-team bij Stichting Optimus is vastgelegd in het IBP-beleidsplan van Stichting Optimus.
Alle meldingen worden opgenomen in het programma: Easy Privacy. PrivacyTeam