stichting carmelcollege

Definitief

Protocol beveiligingsincidenten & datalekken

Inhoud

1. Inleiding

In dit protocol wordt de meldplicht die Stichting Carmelcollege (hierna de Stichting) heeft in het kader van artikel 33 en 34 AVG[1] uitgewerkt. De Stichting is in de zin van de AVG 'verwerkingsverantwoordelijke' voor de verwerking van persoonsgegevens. De Stichting 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 de Stichting omgaat met datalekken en wanneer een datalek vanuit de Stichting wordt gemeld aan de AP. De meldplicht is eveneens van toepassing als het datalek bij een derde is ontstaan, bijvoorbeeld bij een verwerker van persoonsgegevens. Voor verwerkers geldt dat, indien zij geconfronteerd worden met een datalek, zij dit onverwijld aan de vertegenwoordiger van de Stichting moeten doorgeven, zodat deze namens de Stichting de melding kan doen.

Een persoonsgegeven is elk gegeven over een geïdentificeerde of identificeerbare persoon. In het geval van de Stichting gaat het om *leerling- en personeelsgegevens*.

De Stichting 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 De Stichting 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.

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

- **Verwerker** Degene die ten behoeve van de Stichting (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 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. Bv. een verwerker van persoonsgegevens t.b.v. de Stichting (artikel 4 sub 10 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.
- **Persoonsgegeven** Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4 sub 1 AVG).
- **Quick Response Team** Dit is het interne team binnen de Stichting 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: de Stichting.
- **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;
- een computer (systeem) met malware wordt besmet;
- er sprake is van 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).
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.

In **Bijlage 2** 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, moet er een melding plaats te vinden van een datalek aan de AP.
Van een inbreuk die een risico inhoudt voor de rechten en vrijheden van betrokkenen 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 (gezondheids) 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.

[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’.

5. Bepalingen voor de verwerker

Voor verwerkers geldt dat indien zij geconfronteerd worden met een datalek, dit onverwijld aan het bestuursbureau moeten doorgeven, zodat deze namens de Stichting de melding kan doen.

Een verwerker verwerkt persoonsgegevens ten behoeve van de verantwoordelijke (i.c. de Stichting), enkel en alleen op instructie van de verantwoordelijke. De verwerker kan en mag dus zelfstandig niets met de gegevens die hij voor de Stichting verwerkt. De Stichting 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 de Stichting 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. De Stichting 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 de Stichting.
Met deze verwerkers heeft de Stichting 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 AP .
De termijn voor het melden begint te lopen op het moment dat de Stichting 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 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 het bestuursbureau.

6.2. Melding aan betrokkene.

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

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

7. Registratie bijhouden van datalekken

De Stichting houdt een register bij van alle beveiligingsincidenten en van datalekken die onder de meldplicht vallen. Het register valt onder de verantwoordelijkheid van de interne privacy adviseur. 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 De Stichting een mogelijk datalek signaleert, is deze verplicht deze onverwijld intern te melden. De instructie voor medewerkers is te vinden op het intranet van de stichting en…….. […..]. De instructie is opgenomen als bijlage 1.

Hierbij handelt de medewerker als volgt:

1. Het direct na ontdekking opstellen van een mailbericht aan de leidinggevende, de privacycoördinator van de eigen instelling en de interne privacy adviseur van De Stichting (privacy@carmel.nl) , 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.

Na ontvangst van de melding, maakt de privacycoördinator een melding aan in Topdesk.

8.2. Quick Response Team

Vanuit het bestuursbureau wordt een quick response team geformeerd dat aangevuld wordt met de privacycoördinator ven de betreffende instelling. Het Quick Response Team kan zich laten bij staan door interne en externe deskundigen , bijvoorbeeld op het gebied van ICT, communicatie. De leden van het quick response team maken 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.
  Doel: uitzoeken of er sprake is van een beveiligingsincident en/of een datalek.
- Dossier aanmaken (*jaartal en nummer / tijdstip / naam melding*).
- Register Beveiligingsincidenten / Datalekken[4] in Topdesk bijwerken: dossiernummer toevoegen.

[4] Dit register moet minimaal één jaar worden bewaard.

- 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.

- Zo neen: dossier sluiten met duidelijke motivering en conclusie en register bijwerken.
- Zo ja: Quick Response Team meldt aan Management team van het Bestuursbureau.

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;

- moet bewijs veilig gesteld worden;
- 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 persoonsgegevens 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 medewerkers moeten worden betrokken? Denk hierbij aan de verantwoordelijke team- en schoolleiders 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[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.

[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

De interne privacy adviseur (de verantwoordelijke) vult het formulier in en doet de melding aan de Autoriteit Persoonsgegevens. Vóórdat het formulier wordt verzonden vindt er afstemming plaats met het bestuursbureau en de FG. Het College van Bestuur van de Stichting is formeel ‘de melder’. De verantwoordelijkheid voor de communicatie tussen de Stichting en de AP is gedelegeerd naar het bestuursbureau. 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 AP is verzonden, ontvangt de Stichting 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 voor de persoonlijke levenssfeer van betrokkene*? Indien het gaat om medische gegevens, financiële gegevens, BSN, kopie legitimatiebewijs, wordt aangenomen dat dit meestal het geval is.*
- 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 AP.

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 datalekken naar de toekomst toe voorkomen kunnen worden. Deze analyse wordt aan het dossier toegevoegd.
Het dossier en de analyse wordt besproken in het netwerk privacy coördinatoren.

Bijlage 1

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

Binnen de Stichting werken we veel met persoonlijke en dus vertrouwelijke gegevens. Denk hierbij bijvoorbeeld aan leerling gegevens (waaronder gezondheidsgegevens), leerresultaten, personeelsgegevens etc. Al deze informatie is terug te leiden tot een (kwetsbaar) persoon. Hier moeten wij als organisatie natuurlijk zorgvuldig mee omgaan, dat spreekt voor zich.

Een verloren USB stick met informatie over leerlingen die niet encrypted is? Een personeelsdossier in de trein laten liggen? Een computer is gehackt? Een mail met persoonsgegevens is per ongeluk naar een verkeerd mailadres gestuurd? Dit zijn allemaal voorbeelden van datalekken; persoonsgegevens zijn verloren gegaan, liggen ‘op straat’ of zijn niet meer toegankelijk.

De Stichting 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 de Stichting een datalek signaleert, is deze verplicht dit datalek onverwijld te melden.

Hierbij handelt de medewerker als volgt:

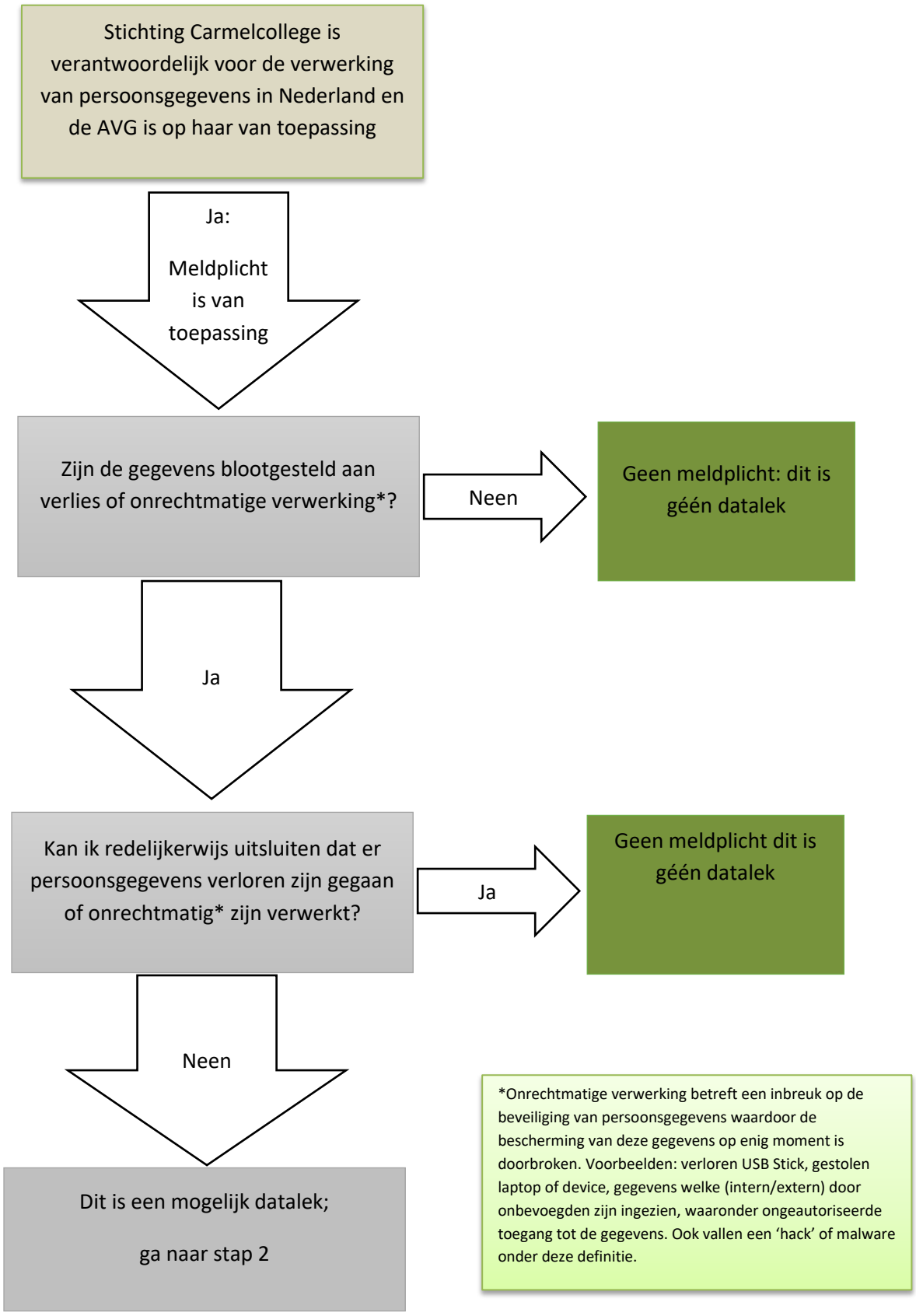
- Hij doet direct na ontdekking van een incident melding hiervan aan de leidinggevende, de privacycoördinator van de eigen instelling en de interne privacy adviseur (privacy@carmel.nl), met daarin een omschrijving van de volgende gegevens:
    - Wat is er precies gebeurd: zo duidelijk mogelijke omschrijving 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.

- Hij verzamelt zo veel mogelijk bewijs en bewaart dit zorgvuldig.

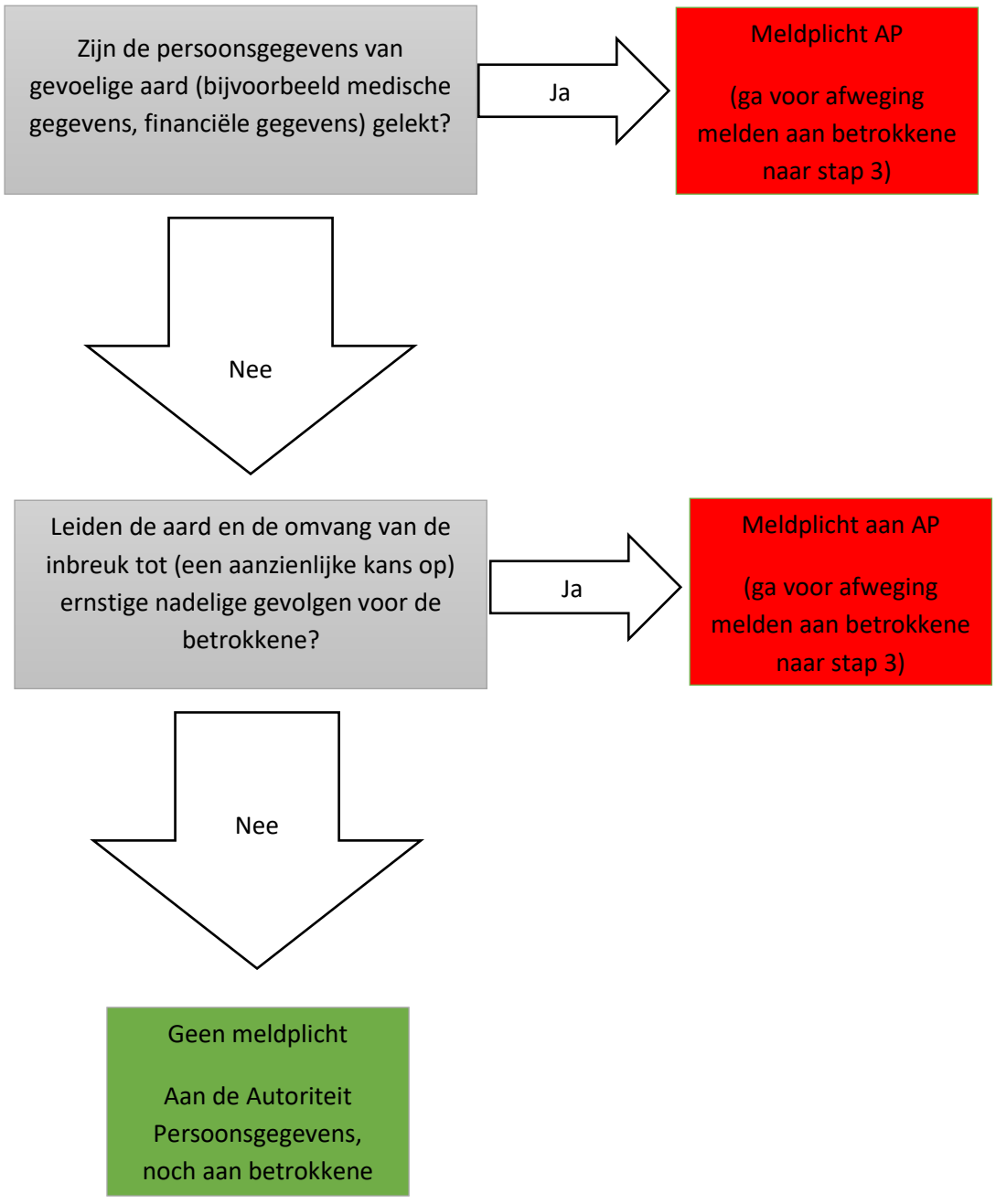
De privacycoördinator zorgt voor melding van het incident in Topdesk

Bijlage 2 Stappenplan datalekken

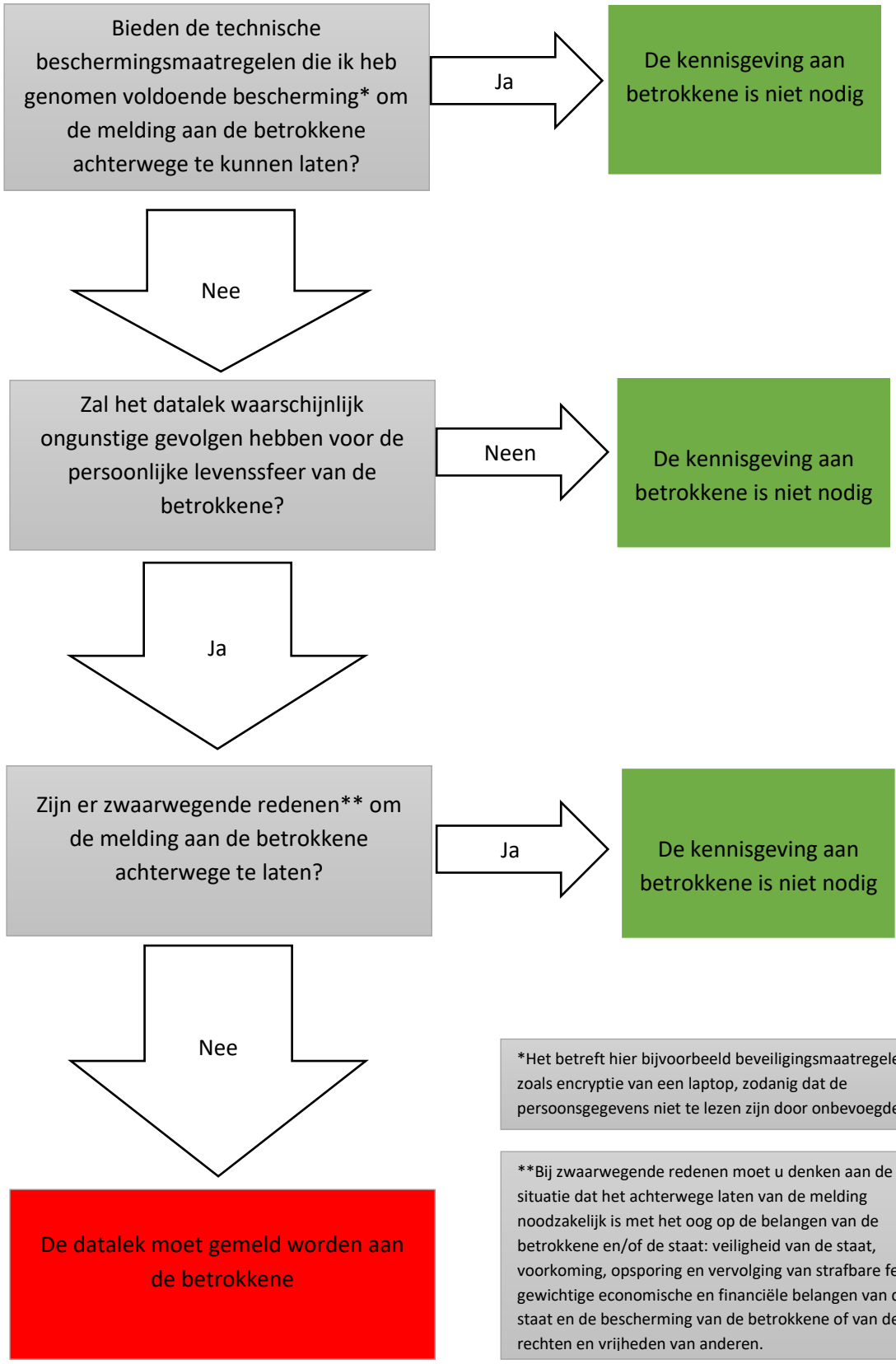
Stap 1: Is het datalek meldingsplichtig richting AP ?



Stap 2: is het waarschijnlijk dat de inbreuk een risico inhoudt voor de rechten en vrijheden van betrokkenen: m.a.w. 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 persoonsgegevens niet te lezen zijn door onbevoegden.

**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.