

Verwerkersovereenkomst Ooijevaar | bevlogen bouwers

Partijen

Bouw- en Aannemingsbedrijf Ooijevaar B.V., ingeschreven bij de Kamer van Koophandel onder nummer 370.38.610, gevestigd aan de Toermalijnstraat 10 te ALKMAAR, ten dezen rechtsgeldig vertegenwoordigd door de heer P.W.L. Vlaar, verder te noemen: **"Verwerkingsverantwoordelijke"**

en

[Statutaire naam bedrijf], ingeschreven bij de Kamer van Koophandel onder nummer [nummer kvk hier invullen], gevestigd aan [straat, huisnummer, plaats], ten dezen rechtsgeldig vertegenwoordigd door [voorletters en naam], verder te noemen: **"Verwerker"**

Hierna gezamenlijk te noemen: **"partijen"**,

in aanmerking nemende dat:

- partijen een overeenkomst met betrekking tot de uitvoering van ontwerp, bouw- en/of onderhoudswerkzaamheden met elkaar hebben gesloten en/of betrokken zijn bij de voorbereiding en uitvoering van bouwwerkzaamheden in de ruimste zin van het woord;
- deze overeenkomst uitsluitend aanvullend en verduidelijkend van aard is op bestaande overeenkomsten en/of werkzaamheden en daarin geen onnodige wijzigingen aanbrengt;
- ter uitvoering van deze werkzaamheden persoonsgegevens worden verstrekt en verwerkt;
- verantwoordelijke grote waarde hecht aan het beschermen van deze persoonsgegevens.

komen partijen in overeenstemming met de AVG overeen dat zij in deze overeenkomst hun afspraken over het verwerken van persoonsgegevens wensen vast te leggen.

1. Definities

De hierna en hiervoor gebruikte begrippen volgen uit de Algemene Verordening Gegevensbescherming en hebben de volgende betekenis:

- 1.1 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de '**Betrokkene**'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
- 1.2 Verwerking: elke handeling / bewerking of geheel van handelingen / bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, bewaren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, samenbrengen, met elkaar in verband brengen, afschermen, wissen of vernietigen van gegevens.
- 1.3 Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen ('Verantwoordelijke').

- 1.4 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt ('Verwerker').
- 1.5 Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie verwerkte persoonsgegevens betrekking hebben.
- 1.6 Verwerkersovereenkomst: deze overeenkomst inclusief de bijlagen ('Verwerkersovereenkomst').
- 1.7 Overeenkomst: de hoofdovereenkomst en/of bouw- en onderhoudswerkzaamheden waar deze verwerkersovereenkomst op toeziet.
- 1.8 Gezamenlijke verantwoordelijkheid: wanneer twee of meer verantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijk verantwoordelijk.
- 1.9 Inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens ('datalek').
- 1.10 Toezichthoudende autoriteit: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens.

2. Voorwerp van de Verwerkersovereenkomst

- 2.1 Verwerker verwerkt in opdracht van Verwerkingsverantwoordelijke – mogelijk doch niet noodzakelijk, noch uitsluitend – de volgende (bijzondere) persoonsgegevens van betrokkenen, welke noodzakelijk zijn ten behoeve van het professioneel, adequaat en klantgericht voorbereiden en uitvoeren van bouw- en/of onderhoudswerkzaamheden welke betrekking hebben op de woning of omgeving van betrokkenen:

- naam en geboortedatum;
- e-mail, telefoonnummer en adresgegevens;
- gezinssamenstelling;
- huisdieren;
- nationaliteit en spreektaal;
- van belang zijnde informatie over gezondheid, zoals invaliditeit en zwangerschap;
- onder bewindvoering en contactgegevens;
- mantelzorg en contactgegevens;
- werktijden en geplande vakanties;
- technische gegevens over uw woning en foto's.

De informatie kan verstrekt worden aan:

- medewerkers of ingehuurde ZZP'ers van Ooijevaar | bevrogen bouwers;
- onderaannemers en leveranciers van Ooijevaar | bevrogen bouwers;
- opdrachtgever en woningeigenaar;
- incidenteel en alleen in noodzakelijke gevallen: hulpdiensten.

Deze informatie mag opgevraagd worden bij:

- Opdrachtgever en woningeigenaar, mits deze daarmee instemmen.

- 2.2 Verwerker verwerkt de persoonsgegevens uitsluitend in het kader van het informeren van en rekening houden met de bewoners in relatie tot de uit te voeren werkzaamheden. Verwerker zal de persoonsgegevens niet voor enig ander doel verwerken.

- 2.3 Verwerker verwerkt de persoonsgegevens volgens de verwerkingshandelingen bestaande uit e-mailberichten, telefoongesprekken, (nieuws)brieven en andere middelen ingezet voor de

communicatie met bewoners/gebruikers/omwonenden en andere belanghebbenden bij het project/de werkzaamheden.

- 2.4 Verwerker zal de persoonsgegevens op behoorlijke, zorgvuldige en transparante wijze en in overeenstemming met de AVG en andere toepasselijke regelgeving verwerken.
- 2.5 Verwerker verwerkt persoonsgegevens in opdracht van Verantwoordelijke en volgt alle instructies van Verantwoordelijke dienaangaande op, behoudens afwijkende wettelijke verplichtingen.
- 2.6 Verwerker heeft geen zeggenschap over de persoonsgegevens verstrekt onder deze verwerkersovereenkomst en neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en de duur van de opslag van gegevens die afwijken van hetgeen is overeengekomen middels deze overeenkomst.
- 2.7 Verwerker mag zonder voorafgaande schriftelijke toestemming van Verantwoordelijke geen andere personen of organisaties inschakelen bij het verwerken van de persoonsgegevens. Verantwoordelijke kan de toestemming om derden in te schakelen aan nadere voorwaarden binden. Wanneer Verwerker met toestemming van Verantwoordelijke andere organisaties inschakelt, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Verwerkersovereenkomst.
- 2.8 Het is verwerker niet toegestaan persoonsgegevens aan anderen dan Verantwoordelijke te verstrekken, tenzij op schriftelijk verzoek van Verantwoordelijke, of met diens schriftelijke toestemming. Verwerker is verplicht schriftelijk te bevestigen dat een verstrekking heeft plaatsgevonden, waarbij hij exact de verstrekte persoonsgegevens, de betrokkene(n), de ontvanger(s) en het moment van verstrekking dient te beschrijven.
- 2.9 Indien verwerker op grond van een wettelijke verplichting gegevens dient te verstrekken, verifieert verwerker de grondslag van het verzoek en de identiteit van de verzoeker en informeert hij onmiddellijk, zo mogelijk voorafgaand aan de verstrekking, Verantwoordelijke terzake.
- 2.10 Verwerker verleent Verantwoordelijke volledige medewerking om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG, meer in het bijzonder de rechten van betrokkenen, zoals een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens, bezwaar maken tegen de verwerking van de persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend bezwaar. Tevens verleent Verwerker volledige medewerking aan het adequaat informeren van de betrokkenen in het kader van de Meldplicht Datalekken.
- 2.11 Indien Verwerker (pogingen tot) onrechtmatige of anderszins ongeautoriseerde verwerkingen of inbreuken op de beveiligingsmaatregelen van de persoonsgegevens signaleert, zal hij Verantwoordelijke hierover onmiddellijk inlichten en op eigen kosten alle redelijkerwijs benodigde maatregelen treffen om (verdere) schending van de AVG of andere regelgeving betreffende de verwerking van de persoonsgegevens, te voorkomen of te beperken een en ander onverminderd de verplichting van Verwerker om de eventueel door Verantwoordelijke daardoor geleden schade te vergoeden.
- 2.12 Indien Verwerker een datalek signaleert zoals bedoeld in art. 34a lid 1. van de Wbp, zal hij dit datalek onverwijld melden bij Verantwoordelijke. Verwerker meldt het datalek bij de Autoriteit persoonsgegevens (AP) volgens wettelijk voorgeschreven standaarden en binnen wettelijk gestelde tijd en stuurt een kopie van de melding aan Verantwoordelijke t.a.v. de contactpersoon bij Verantwoordelijke en met kopie aan de privacy officer. Het staat de Verantwoordelijke vrij om de melding aan te passen en de aanpassingen na te sturen aan AP. De Verantwoordelijke informeert de betrokkenen over het datalek.

- 2.13 In geval van de ontdekking van een mogelijk datalek zal Verwerker Verantwoordelijke hierover informeren binnen een termijn van 24 uur overeenkomstig het proces volgens uit Bijlage 2, zodat Verantwoordelijke indien nodig een melding van het datalek bij de Toezichthouder kan doen en betrokkenen eventueel op de hoogte kan stellen.
- 2.14 Verwerker zal Verantwoordelijke op de hoogte houden van nieuwe ontwikkelingen rondom het datalek, ook zal Verwerker de getroffen maatregelen om het datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen, overleggen aan Verantwoordelijke.
- 2.15 Verantwoordelijke en Verwerker zorgen ervoor dat de functionaris voor de gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.
- 2.16 De overgebleven persoonsgegevens zal Verwerker vernietigen zodra de gegevens niet meer noodzakelijk zijn voor het uitvoeren van de werkzaamheden, dan wel na verstrijken van de wettelijke bewaartermijn (hierbij valt bijvoorbeeld te denken aan persoonsgegevens die om belastingtechnische redenen bewaard moeten blijven), dan wel op verzoek van Verantwoordelijke.

3. Beveiliging

- 3.1 Verwerker zorgt ervoor dat de persoonsgegevens voldoende worden beveiligd. Om verlies en onrechtmatige verwerkingen te voorkomen neemt Verwerker passende technische en organisatorische maatregelen (een overzicht van mogelijke maatregelen en het beleid daaromtrent is opgenomen in Bijlage 1 bij deze overeenkomst). Deze maatregelen zijn afgestemd op het risico van de Verwerking. Verwerker garandeert een beveiligingsniveau dat voldoet aan de AVG en het in artikel 13 Wet bescherming persoonsgegevens vereiste beschermingsniveau.
- 3.2 Verwerker verwerkt geen persoonsgegevens buiten een land van de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Verantwoordelijke.
- 3.3 Wanneer een der partijen vindt dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden partijen in overleg over de wijziging daarvan. De kosten die gemoeid gaan met het wijzigen van de beveiligingsmaatregelen komen voor rekening van degene die de kosten maakt.

4. Geheimhouding

- 4.1 Verwerker is gehouden tot geheimhouding van alle persoonsgegevens en informatie die zij als uitvloeisel van deze Verwerkerovereenkomst verwerkt, behoudens in zoverre die gegevens of informatie klaarblijkelijk geen geheim of vertrouwelijk karakter hebben, algemeen bekend zijn, of geheimhouding op basis van een wettelijke verplichting niet kan.
- 4.2 Verwerker zorgt dat zijn/haar personeel en ingeschakelde hulppersonen zich aan deze geheimhouding houden, door een geheimhoudingsplicht in de (arbeids-)contracten op te nemen.
- 4.3 Indien Verantwoordelijke daarom uitdrukkelijk schriftelijk verzoekt, zal Verwerker ten aanzien van aangeduide gegevens of informatie bijzondere maatregelen treffen met het oog op de geheimhouding daarvan, welke maatregelen onder meer kunnen inhouden de vernietiging van betrokken gegevens of informatie zodra de noodzaak voor Verwerker om daarvan nog langer kennis te nemen, is komen te vervallen.
- 4.4 Verwerker verplicht zich om personen die door haar worden ingezet bij de uitvoering van deze overeenkomst dezelfde verplichting op te leggen als in het eerste lid van dit artikel is opgenomen.

4.5 Na afloop van de werkzaamheden of overeenkomst en deze verwerkersovereenkomst blijft dit artikel 4 en de hierin besproken geheimhouding van kracht.

4.6 Partijen zullen over en weer strikte geheimhouding in acht nemen ten aanzien van eventuele beveiligingsincidenten.

5. Controle

5.1 Verantwoordelijke behoudt zich het recht voor een audit uit te laten voeren om te bepalen of het verwerken van de persoonsgegevens aan de wet en de afspraken uit deze Verwerkersovereenkomst voldoet. Verwerker zal alle benodigde medewerking verlenen aan de controle en ervoor zorgdragen dat ook de door hem ingeschakelde derden hiertoe de benodigde medewerking zullen verlenen.

5.2 Het uitvoeren van een controle zal niet tot een vertraging van de door Verwerker in het kader van de overeenkomst en deze Verwerkersovereenkomst te verrichten werkzaamheden mogen leiden. Indien dat onverhoopt toch het geval is, zullen oartijen in overleg treden teneinde daarvoor zo snel mogelijk een oplossing te vinden.

5.3 Controle op de algehele verwerking van persoonsgegevens door Verwerker kan, naast de auditmogelijkheid, ook geschieden via zelfevaluatie door Verwerker. Verwerker zal hierbij aan Verantwoordelijke een rapport verstrekken waarin Verwerker aantoont dat hij voldoet aan de wet en de afspraken uit deze Verwerkersovereenkomst. Deze rapportage dient te worden ondertekend door een directielid binnen de organisatie van Verwerker.

5.4 Verwerker voert de door Verantwoordelijke aangegeven aanbevelingen ter verbetering uit binnen de daartoe door Verantwoordelijke te bepalen termijn.

6. Aansprakelijkheid

6.1 Verwerker is jegens Verantwoordelijke volledig aansprakelijk voor alle directe en indirecte schade die voortvloeit uit enige tekortkomingen van Verwerker in de nakoming van haar verplichting uit hoofde van de wet en deze overeenkomst.

6.2 Verwerker zal Verantwoordelijke vrijwaren tegen en schadeloos houden voor alle aanspraken van derden die ontstaan als gevolg van, of die verband houden met, een werkelijke of vermeende schending van toepasselijke wet- en regelgeving en gedragscodes terzake van de bescherming van persoonsgegevens, waaronder in ieder geval mede begrepen de AVG.

6.3 Verwerker is aansprakelijk voor de eventueel aan Verantwoordelijke opgelegde bestuurlijke boete door de Toezichthouder als de schade het gevolg is van het onrechtmatig of nalatig handelen van Verwerker. Verantwoordelijke is niet aansprakelijk voor aanspraken van Betrokkenen of andere personen en organisaties waar Verwerker de samenwerking mee is aangegaan of waarvan Verwerker persoonsgegevens verwerkt, als dit het gevolg is van het onrechtmatig of nalatig handelen van Verwerker.

7. Totstandkoming, duur en einde van de Verwerkersovereenkomst

7.1 Deze Verwerkersovereenkomst treedt in werking op de datum dat partijen de Overeenkomst hebben ondertekend.

7.2 Deze Verwerkersovereenkomst zal van kracht zijn gedurende de periode dat verwerker in het kader van uit te voeren of uitgevoerde bouw- en/of onderhoudswerkzaamheden beschikt over persoonsgegevens van betrokkenen.

7.3 Na beëindiging van deze Verwerkersovereenkomst zullen de lopende verplichtingen voor Verwerker, zoals het melden van Datalekken waarbij Persoonsgegevens van Verantwoordelijke betrokken zijn en de plicht tot geheimhouding blijven voortduren.

8. Slotbepaling

8.1 Wijziging van deze overeenkomst of aanvullingen daarop zijn slechts geldig indien deze schriftelijk zijn overeengekomen in een door beide partijen ondertekende (al dan niet in briefvorm opgestelde) wijzigingsovereenkomst.

8.2 Eventuele geschillen in het kader van deze overeenkomst worden voorgelegd aan de rechtbank te Amsterdam.

8.3 Indien de wetgeving met betrekking tot de privacy en/of bescherming van persoonsgegevens wijzigt, zullen partijen meewerken om deze Verwerkersovereenkomst aan te passen, teneinde aan de van toepassing zijnde wetgeving te blijven voldoen.

8.4 Deze Verwerkersovereenkomst vormt een aanvulling op eventuele andere overeenkomsten. Bij conflicterende bepalingen uit deze Verwerkersovereenkomst en andere overeenkomsten prevaleren de bepalingen uit deze Verwerkersovereenkomst.

Aldus overeengekomen en ondertekend in tweevoud

Handtekening Ooijevaar:

.....

Naam:

Functie:.....

Datum:

Handtekening Verwerker:

.....

Naam:

Functie:.....

Datum:

Bijlage 1: Overzicht met beveiligingsmaatregelen

Om vast te stellen wat passende beveiligingsmaatregelen zijn, moet een afweging worden gemaakt op basis van de risico's van de verwerking aan de hand van onder meer de volgende punten:

- het soort persoonsgegevens dat verwerkt wordt (normaal, bijzonder of gevoelig) en eventueel de daarbij behorende (risico)classificatie die de organisatie zelf aan de gegevens heeft gegeven. *Gaat het bijvoorbeeld om een naam of een e-mailadres, wat minder gevoelige Persoonsgegevens zijn, of gaat het om het verwerken van een BSN;*
- de hoeveelheid betrokkenen van wie gegevens worden verwerkt. *Hoe meer betrokkenen er zijn, hoe meer eisen er worden gesteld aan de beveiliging van de gegevens;*
- het doel waarvoor gegevens worden verwerkt;
- de duur en de wijze waarop gegevens bewaard moeten worden.

Er kan vervolgens onderscheid gemaakt worden tussen organisatorische beveiligingseisen, zoals het voorkomen van diefstal van een laptop met daarop persoonsgegevens uit de auto, en technische beveiligingseisen, zoals een uitgebreide IT-omgeving die beveiligd wordt tegen virussen en waar encryptie van de gegevens wordt toegepast.

De onderstaande maatregelen zijn suggesties voor beveiligingsmaatregelen en de aanwezigheid hiervan kan een indicatie zijn van een gepast beveiligingsniveau.

Technische beveiligingsmaatregelen

- Up-to-date virusscanner op elke laptop, PC en tablet
- Beveiligde USB-sticks
- Accurate beveiliging medewerkerstelefoon
- Bitlocker toegangsmechanisme
- Unieke inlogcode en wachtwoord (regelmatig aanpassen)
- Versleutelde e-mail
- Geen onbeveiligde externe harde schijven
- Geen onbeveiligde back-ups maken
- Geen documenten op privé-laptop opslaan

Organisatorische beveiligingsmaatregelen

- Clean desk policy
- Laptop niet onbemand achterlaten
- Laptop nooit achterlaten in de auto
- Privacyscreens medewerkers
- Oude documenten op juiste manier vernietigen
- Zorgvuldig gebruik van USB-sticks

Bijlage 2

Proces voor het melden van datalekken en de te verstrekken informatie

Wat is een beveiligingsincident en wanneer moet dit gemeld worden? Een datalek is een beveiligingsincident waarbij persoonsgegevens, die de Verwerker namens de Verantwoordelijke beheert, mogelijk verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. Het gaat om gegevens die te koppelen zijn aan deze personen, zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, e-mailadressen, login-gegevens, cookies, IP-adressen of identificerende gegevens van computers of telefoons.

Hieronder vindt u een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens.

- De website met login-gegevens is gehackt of is toegankelijk voor derden.
- Verlies van een laptop of USB-stick met persoonsgegevens.
- Salarisstroken van medewerkers zijn per ongeluk naar verkeerde personen gestuurd.
- Brieven of e-mails worden naar een verkeerd adres gestuurd.
- Een aanval van een hacker op het ICT-systeem.
- Een verloren of gestolen telefoon waar persoonsgegevens op aanwezig zijn.

Wat te doen bij twijfel?

Als je op basis van bovenstaande niet zeker weet of er sprake is van een beveiligingsincident, stel je jezelf in ieder geval alvast de volgende vragen als hulpmiddel:

- Is er een technisch of fysiek beveiligingsprobleem?
- Gaat het probleem over de beveiliging van Persoonsgegevens? Ook IP-adressen, telefoonnummers of identificerende gegevens, bijvoorbeeld van hardware, kunnen hieronder vallen.
- Gaat het om gevoelige gegevens zoals ras, gezondheidsgegevens, informatie over iemands financiële situatie zoals salaris of gegevens waar (identiteits)fraude mee kan worden gepleegd, zoals een Burgerservicenummer?
- Zijn er grote hoeveelheden persoonsgegevens onbedoeld toegankelijk geworden voor derden?
- Gaat het om gegevens van kwetsbare groepen zoals kinderen?
- Worden de persoonsgegevens beheerd door een leverancier?

Ook wanneer je twijfelt, neem het zekere voor het onzekere en neem altijd contact op met de Verwerkingsverantwoordelijke. Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met Margret Dekker van Ooijevaar | bevlogen bouwers. Telefoon: 072-511 86 96, e-mail: M.Dekker@ooijevaar.nl

Geef in je e-mail alvast antwoorden op de onderstaande vragen. Deze vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt. Gaarne onderstaande vragen zo volledig mogelijk en schriftelijk beantwoorden:

1. Geef een samenvatting van het beveiligingslek/beveiligingsincident/datalek: wat is er gebeurd? Vermeld hier ook de naam van het betrokken systeem.
2. Welke typen persoonsgegevens zijn betrokken bij het beveiligingsincident? Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.
3. Van hoeveel personen zijn de persoonsgegevens betrokken bij het beveiligingsincident? Geef a.u.b. een minimum en maximum aantal personen.

4. Omschrijving groep personen om wiens gegevens het gaat. Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van een kwetsbare groepen personen zoals kinderen, ouderen en zieken.
5. Zijn de contactgegevens van de betrokken personen bekend? Het kan zijn dat betrokkenen geïnformeerd moeten worden over het datalek. Hoe kunnen we deze personen in dat geval bereiken?
6. Wat is de oorzaak (root cause) van het beveiligingsincident? Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan? Graag zo nauwkeurig mogelijk beschrijven.
7. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden? Geef dit a.u.b. zo specifiek mogelijk aan.