Verwerkersovereenkomst

Verwerkersovereenkomst

Datum:

Contractspartijen:

1. Verantwoordelijke te weten _____, statutair gevestigd te _____, vertegenwoordigd door _____ hierna te noemen: "Verantwoordelijke", en
2. Verwerker te weten LEAD Solutions BV, statutair gevestigd te Utrecht, vertegenwoordigd door ir. J.G.M. Wijntjes, hierna te noemen: "Verwerker",
3. gezamenlijk aan te duiden als: "Wij";

Overwegende dat:

Wij hebben een overeenkomst met betrekking tot de implementatie en onderhoud van Carta Cursusadministratie gesloten. Ter uitvoering van onze Overeenkomst worden Persoonsgegevens verwerkt.

Verantwoordelijke hecht grote waarde aan het beschermen van deze Persoonsgegevens, daarom is Verantwoordelijke verantwoordelijk voor de gegevens die Verwerker gaat verwerken en leggen Wij in deze Verwerkersovereenkomst en de daarbij behorende bijlagen vast wat Verwerker wel en niet mag doen met de Persoonsgegevens.

Bijlagen:

1. Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen

2. Overzicht met beveiligingsmaatregelen

3. Proces rondom het melden van Datalekken en de te verstrekken informatie

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": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, 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 lidstatelijk 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;

1.5 “Betrokkene”: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte persoonsgegevens betrekking hebben;

1.6 “Verwerkersovereenkomst”: deze overeenkomst inclusief de bijlagen;

1.7 “Overeenkomst”: de hoofdovereenkomst waar deze Verwerkersovereenkomst uit voortvloeit;

1.8 “Datalek”: 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;

1.9 “Gegevensbeschermingseffectbeoordeling”: het uitvoeren van een beoordeling, voorafgaand aan het uitvoeren van de verwerking, van het effect van de beoogde verwerkingsactiviteiten op de bescherming van de persoonsgegevens.

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 Totstandkoming, duur en beëindiging van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst treedt in werking op de datum waarop Wij deze ondertekenen.

2.2 Deze Verwerkersovereenkomst wordt onderdeel van de Overeenkomst en zal gelden voor zolang de Overeenkomst duurt.

2.3 Indien de Overeenkomst eindigt, eindigt deze Verwerkersovereenkomst automatisch; de Verwerkersovereenkomst kan niet apart worden opgezegd.

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

3 Verwerken Persoonsgegevens

3.1 Verwerker zal alleen Persoonsgegevens verwerken in opdracht van Verantwoordelijke en heeft geen zeggenschap over de Persoonsgegevens. Verwerker volgt de instructies van Verantwoordelijke hierover op en Verwerker mag de Persoonsgegevens niet op een andere manier verwerken, tenzij Verantwoordelijke Verwerker daar van te voren toestemming of opdracht voor geeft.

3.2 In Bijlage 1 wordt opgenomen welke Persoonsgegevens Verwerker precies zal verwerken en voor welke verwerkingsdoeleinden.

3.3 Verwerker houdt zich aan de wet en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze.

3.4 Verwerker maakt gebruik van diensten van vertegenwoordigers, consultants en serviceproviders die namens Verwerker Persoonsgegevens verwerken om bepaalde bedrijf gerelateerde functies uit te voeren.

De bedrijven die hiervoor worden ingeschakeld zijn, voor zover mogelijk, opgenomen in de verwerkingsdoeleinden in Bijlage 1

3.5 Verwerker kan andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens indien dit voor de uitvoering van de overeenkomst door verwerker noodzakelijk wordt geacht.

3.6 Wanneer Verwerker andere organisaties inschakelt, moeten deze minimaal voldoen aan de eisen die zijn opgenomen in deze Verwerkersovereenkomst.

3.7 Verantwoordelijk kan op verzoek op ieder moment inzage vragen in de actuele lijst van deze organisaties. Verantwoordelijke kan bij Verwerker bezwaar maken indien Verantwoordelijk de wens heeft een Verwerking niet bij de door de Verwerker geselecteerde organisatie te laten uitvoeren.

3.8 Wanneer Verantwoordelijke een verzoek krijgt van een Betrokkene die zijn of haar privacy rechten wil uitoefenen, werkt Verwerker daar binnen een termijn van 14 dagen aan mee. Deze rechten bestaan uit een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van de Persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens.

3.9 Wanneer Verantwoordelijke Verwerker verzoekt om Verantwoordelijke informatie te geven, dan zal Verwerker de informatie verstrekken die Verantwoordelijke nodig heeft voor het uitvoeren van een Gegevensbeschermingseffectbeoordeling. Verantwoordelijke heeft dit nodig om in te kunnen schatten wat het risico van de Verwerking is die Verwerker namens Verantwoordelijke uitvoert.

4 Beveiligen van Persoonsgegevens

4.1 Verwerker zal de Persoonsgegevens voldoende beveiligen. Om verlies en onrechtmatige verwerkingen te voorkomen neem Verwerker passende technische en organisatorische maatregelen.

4.2 Deze maatregelen zijn afgestemd op het risico van de verwerking. Een overzicht van deze maatregelen en het beleid daarover is opgenomen in Bijlage 2.

4.3 Ter controle zal Verwerker aan Verantwoordelijke jaarlijks een rapportage ter beschikking stellen met daarin de genomen beveiligingsmaatregelen en de eventuele aandachts- en/of verbeterpunten. Hiervoor zal Verwerker aan Verantwoordelijke geen extra kosten in rekening brengen.

4.4 Verantwoordelijke mag een inspectie of audit in de organisatie van Verwerker laten uitvoeren om te bepalen of het verwerken van de Persoonsgegevens aan de wet en de afspraken uit deze Verwerkersovereenkomst voldoet. Hierbij zal Verwerker aan Verantwoordelijke medewerking verlenen, waaronder het ter beschikking stellen van alle relevante informatie.

4.5 De kosten voor de uitvoering van deze audit zullen voor rekening van Verwerker komen wanneer blijkt dat Verwerker zich niet aan de verplichtingen in deze Verwerkersovereenkomst houdt.

4.6 De controle op de algehele verwerking van Persoonsgegevens door Verwerker kan, naast de audit mogelijkheid, ook gebeuren via zelfevaluatie. Verwerker zal hierbij aan Verantwoordelijke een rapport verstrekken waarin Verwerker aantoont dat Verwerker voldoet aan de wet en de afspraken uit deze Verwerkersovereenkomst. Deze rapportage dient te worden ondertekend door een directielid binnen de organisatie van Verwerker. (al in 4.3)

4.7 Wanneer Verwerker of Verantwoordelijke vindt dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden Wij in overleg over de wijziging daarvan. De kosten voor het wijzigen van de beveiligingsmaatregelen komen voor rekening van degene die de kosten maakt.

5 Exporteren Persoonsgegevens

5.1 Verwerker mag geen Persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER), zonder daarvoor voorafgaande schriftelijke toestemming te hebben verkregen van Verantwoordelijke.

6 Geheimhouding

6.1 Verwerker zal de aan Verwerker verstrekte Persoonsgegevens geheimhouden, tenzij dit op basis van een wettelijke verplichting niet mogelijk is.

6.2 Verwerker zal ervoor zorgen dat ook het personeel van Verwerker en ingeschakelde hulppersonen zich aan deze geheimhouding houden, door een geheimhoudingsplicht in de (arbeids-) contracten op te nemen.

7 Datalekken

7.1 In geval van een ontdekking van een mogelijk Datalek zal Verwerker Verantwoordelijke hierover binnen 24 uur informeren en aan Verantwoordelijke de informatie verstrekken die is aangegeven in Bijlage 3, zodat Verantwoordelijke indien nodig een melding bij de Toezichthouder kan doen.

7.2 Na de melding van een Datalek aan Verantwoordelijke zal Verwerker Verantwoordelijke op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek en de maatregelen die Verwerker heeft getroffen om de omvang van het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen.

7.3 Het is niet toegestaan dat Verwerker een melding van een Datalek doet aan de Toezichthouder en ook mag Verwerker de Betrokkenen niet informeren over het Datalek. Dit is de verantwoordelijkheid van de Verantwoordelijke.

7.4 Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van degene die de kosten maakt.

8 Aansprakelijkheid

8.1 Als Verwerker de verplichtingen van Verantwoordelijke uit deze Verwerkersovereenkomst niet nakomt, stelt Verantwoordelijke de Verwerker daarvoor aansprakelijk.

8.2 Verwerker is aansprakelijk voor alle schade geleden door het niet nakomen van de wet en de bepalingen uit deze Verwerkersovereenkomst, voor zover dit is ontstaan door werkzaamheden van Verwerker.

8.3 Verwerker is aansprakelijk voor de aan Verantwoordelijke opgelegde bestuurlijke boete door de Toezichthouder als de geleden schade het gevolg is van onrechtmatig of nalatig handelen door Verwerker.

8.4 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 onrechtmatig of nalatig handelen van Verwerker.

8.5 Verwerker 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 onrechtmatig of nalatig handelen van Verantwoordelijke.

9 Teruggave Persoonsgegevens en bewaartermijn

9.1 Na het beëindigen van deze Verwerkersovereenkomst zal verwerker eventuele achter gebleven Persoonsgegevens op een zorgvuldige en veilige manier verwijderen.

9.2 Verwijderde persoonsgegevens kunnen voor een verdere periode blijven bestaan op back-up- of archiefmedia om juridische, wettelijke of belastingredenen, of om legitieme en wettige zakelijke doeleinden.

9.3 Verwerker zal op verzoek na de teruggave en/of verwijdering van de Persoonsgegevens schriftelijk aan Verantwoordelijke een verklaring betreffende de status van de Persoonsgegevens doen.

10 Slotbepalingen

10.1 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op de Verwerkersovereenkomst.

10.2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de Verwerkersovereenkomst en de Overeenkomst, gelden de bepalingen uit deze Verwerkersovereenkomst.

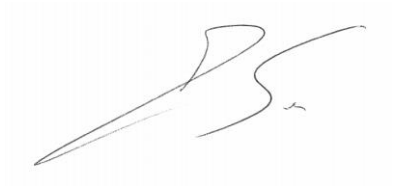
10.3 Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig wanneer Wij dit samen schriftelijk afspreken.

10.4 Op deze Verwerkersovereenkomst en werkzaamheden door Verwerker is het Nederlandse recht van toepassing.

10.5 Over eventuele geschillen tussen Verwerker en Verantwoordelijke bepaalt de rechter in de rechtbank van Utrecht.

11 Ondertekening

Aldus overeengekomen en ondertekend:

Verantwoordelijke	Verwerker
Ondertekend voor en namens:	Ondertekend voor en namens:
	LEAD Solutions BV
……	
Naam:	Naam:
	Hans Wijntjes
……	
Functie:	Functie:
	Directeur
……	
Datum en plaats:	Datum en plaats:
……	2 mei 2018
Handtekening:	Handtekening:
……	

Bijlage 1. Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen

Hieronder een volledig overzicht van de persoonsgegevens die verwerkt zullen worden.

Soorten Betrokkenen
- Cursisten en geïnteresseerden.
- Docenten
- Medewerkers van Verantwoordelijke
- Medewerkers van klanten van Verantwoordelijke
- Leveranciers van Verantwoordelijke

Verwerkte persoonsgegevens.

Naam	adresgegevens	competenties*
telefoonnummer(s) *	e-mailadres(sen)	opleiding en interesses
geboortedatum**	relatienummer	geslacht
burgerlijke staat*	studieresultaten	IBAN***
Foto*	BSN**	Betaalgegevens***
Functie/positie in bedrijf*		

De met * gemarkeerde gegevens zijn niet verplicht om te registreren. Het is aan Verantwoordelijke om hierover te beslissen.
De met ** gemarkeerde gegevens zijn in het algemeen niet verplicht om te registreren. Voor sommige verwerkingen (zoals officiële getuigschriften/diploma's) zijn deze gegevens echter noodzakelijk voor het verwerkingsdoel.
De met *** gemarkeerde gegevens zijn in het algemeen niet verplicht om te registreren. Registratie is alleen noodzakelijk wanneer Verantwoordelijke het systeem ook voor financiële verwerking inzet.

Beschrijving verwerkingsactiviteiten door Verwerker:
Leveren van een cursusadministratiesysteem
Verwerkingsdoelen:
- Ondersteuning bij het inrichten, gebruik en verwerking van gegevens t.b.v. cursusadministratie.
- Oplossen van incidenten die in het cursusadministratie systeem optreden
- Uitwisseling van gegevens met financiële systemen (facturatie/betaling/bank)
- Uitwisseling van gegevens met marktpartijen (e-mail van resultaten, getuigschrift, planning etc.).
- Uitwisseling van gegevens met werkgever cursisten (aanwezigheid, resultaten)

Verwerkingsverantwoordelijke: Hans Wijntjes

Voor de verwerking van Persoonsgegevens kunnen de volgende verwerkers worden ingeschakeld:

- Interne en externe medewerkers.
    - Realiseren van verbeteringen aan de software
    - Analyse van de werking van de software.
    - Onderzoek van gemelde problemen.

Afhankelijk van het type hosting waarvoor Verantwoordelijke tijdens de implementatie voor heeft gekozen, zijn een aantal van de hieronder genoemde providers betrokken bij de verwerking van persoonsgegevens van de Verwerker.

Verantwoordelijke maakt gebruik van onderstaande hostingsconfiguratie:

Welke gegevens	Hosting type	Onderdeel dienstenpakket Verantwoordelijke
Database1	DataCloud	Ja / Nee
Database2	Carta Online	Ja / Nee
Sjablonen en Archief	DataCloud	Ja / Nee
Backups	Carta	Ja / Nee
Email	Transactional	Ja / Nee
Database3	Carta365 DB	Ja / Nee
Sjablonen en Archief	Carta365	Ja / Nee
Email	Carta365 Mail	Ja / Nee

Hosting Carta

Interne opslag bij Verwerker

Externe hosting

Hosting Datacloud en Carta Online

Naam bedrijf: KPN InternedServices
Contact: 0299 - 476 185
E-mail: info@internedservices.nl | abuse@internedservices.nl
Locatie: Wielingenstraat 8, 1441 ZR Purmerend

Hosting Transactional:

Naam bedrijf: The Rocket Science Group LLC d/b/a MailChimp
Contact: Daniel Kurzius
Title: CCO/Co-founder

Hosting Carta365, Carta365 DB en Carta365 Mail

Naam bedrijf: Micros internetdientsten
Contact: Frans Poldervaart
Tel: 010-2450333
E-mail: support@microsinternetdiensten.nl

Bijlage 2. Overzicht met beveiligingsmaatregelen

Over het algemeen willen we niet graag veel informatie over onze beveiligingspraktijken bekendmaken, omdat dit alleen de mensen helpt waar we ons tegen beveiligen. Maar we realiseren ons dat beveiliging belangrijk voor u is. Daarom hebben we besloten antwoorden te plaatsen op de vragen die volgens ons het belangrijkst zijn voor onze klanten.

Bescherming tegen gegevensverlies, corruptie

Alle klantdatabases worden gescheiden gehouden. Hierdoor is het onmogelijk dat u per ongeluk informatie van andere klanten kunt benaderen. Bijkomend voordeel is dat de integriteit beter gewaarborgd kan worden. Gratis gebruikersaccounts worden in 1 database geplaatst. Als de gratis accounts te veel data bevatten, worden ze gemigreerd naar hun eigen afzonderlijke databases.

Beveiliging op applicatieniveau

Carta Online wachtwoorden zijn gehasht. Onze eigen medewerkers kunnen ze niet eens bekijken. Wanneer u uw wachtwoord verliest, kan het niet worden opgehaald. Het moet worden gereset.

Alle pagina's van onze websites, klantwebsites en inschrijfpagina’s geven gegevens door via SSL. Voor productieomgevingen wordt dit afgedwongen, voor test en acceptatieomgevingen is zowel https als http toegang mogelijk.

Inlogpagina's hebben brute force-beveiliging.

Aanmeldingen via de Carta Online API hebben brute force-beveiliging.

Interne IT-beveiliging

Het Carta Online kantoor is centraal beveiligd. Individuele kantoorruimtes worden afgesloten wanneer niemand zich in de ruimte bevindt. Het gebouw beschikt over camerabewaking en buiten kantooruren is een alarm gebaseerd op bewegingsdetectie actief.

Intern protocol en opleiding

Wij verplichten onze medewerkers wachtwoorden te gebruiken van minimaal 12 random gegenereerde karakters en nooit twee keer hetzelfde wachtwoord te gebruiken voor verschillende systemen. Veiligheid wordt echter niet gegarandeerd door dit soort procedures. Veiligheid kun je alleen goed nastreven wanneer men de onveilige situaties herkent. Daarom trainen wij onze medewerkers niet alleen in het correct gebruik van wachtwoorden en tokens. We leren ze ook het een en ander over het hacken van computersystemen. Het boek ‘The art of invisibility’ van Kevin Mitnick is verplichte lectuur voor nieuwe werknemers.

Bijlage 3: Proces rondom het melden van Datalekken en de te verstrekken informatie

Wat is een datalek en wanneer moet dit gemeld worden?

Een datalek is een beveiligingsincident waarbij Persoonsgegevens, die de Verwerker namens de

Verwerkingsverantwoordelijke 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, log in gegevens, cookies, IP adressen of identificerende gegevens van computers of telefoons.

Hieronder vind je een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens.

- De website met logingegevens is gehackt of is toegankelijk voor derden.

- Verlies van een laptop of USB-stick met persoonsgegevens.

- Brieven of e-mails worden naar een verkeerd adres gestuurd.

- Een aanval van een hacker op het ICT systeem.

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 Verwerker.

Waar meld je het beveiligingsincident?

Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met de Verwerker

TEL: 085 303 26 77

En via

E-MAIL: datalek@cartaonline.nl

Geef in je e-mail beantwoording op de onderstaande vragen.

Wij willen graag dat je de onderstaande vragen voor ons beantwoord. Deze vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt.

De Verwerker kan je helpen met de beantwoording hiervan. Gaarne de 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.

5. Zijn de contactgegevens van de betrokken personen bekend?

Het kan zijn dat betrokkenen geïnformeerd moeten worden over het datalek, 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?

7. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden? Geef dit a.u.b. zo specifiek mogelijk aan.