VERWERKERSOVEREENKOMST

Partijen:

1. Your Signature, statutair gevestigd te DEN HAAG , in deze rechtsgeldig vertegenwoordigd door A Zengin Smit, hierna nader te noemen: "Verwerkingsverantwoordelijke";

en

2. Netbase B.V., handelend onder de naam WebReus, statutair gevestigd aan de (5652 AB) Beemdstraat 14 te Eindhoven en geregistreerd bij de KvK onder het nummer: 17079744, in deze rechtsgeldig vertegenwoordigd door haar algemeen directeur, hierna nader te noemen: "Verwerker";

hierna gezamenlijk te noemen: ‘Partijen’

OVERWEGENDE DAT

A. Verwerkingsverantwoordelijke en Verwerker een overeenkomst hebben gesloten op 2018-10-04 15:50:47, hierna de "Overeenkomst". Deze Overeenkomst heeft betrekking op het leveren van diensten aan Verwerkingsverantwoordelijke zoals beschreven in Bijlage 1.

B. Verwerker in de uitvoering van de Overeenkomst en de levering van Diensten aan Verwerkingsverantwoordelijke Persoonsgegevens Verwerkt voor Verwerkingsverantwoordelijke;

C. Verwerkingsverantwoordelijke en Verwerker beschouwen de correcte naleving van de privacywetgeving, alsmede de correcte Verwerking van Persoonsgegevens als uiterst belangrijk;

D. Partijen met deze Verwerkersovereenkomst invulling willen geven aan de wijze van Verwerking van Persoonsgegevens door Verwerker;

E. De bepalingen in deze Verwerkersovereenkomst gaan voor op alle andere afspraken die tussen Partijen gelden en betrekking hebben op de Verwerking van Persoonsgegevens door Verwerker voor Verwerkingsverantwoordelijke.

KOMEN ALS VOLGT OVEREEN:

1. Definities

1.1 De volgende termen hebben de volgende betekenis:

AP	Autoriteit Persoonsgegevens, ook wel College Bescherming Persoonsgegevens genoemd, de toezichthoudende autoriteit voor de naleving van de privacyregelgeving in Nederland;
AVG	de algemene verordening gegevensbescherming. Deze verordening is per 25 mei 2018 van toepassing en vervangt per die datum de tot dan in Nederland geldende Wet bescherming persoonsgegevens (Wbp);
Betrokkene	de natuurlijke persoon waarop de Persoonsgegevens die Partijen Verwerken in het kader van de uitvoering van de Overeenkomst betrekking hebben (artikel 4 sub 1 AVG);
Beveiligingsincident	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 (artikel 4 sub 12 AVG);
Bijlage	iedere bijlage bij deze Verwerkersovereenkomst, welke een onlosmakelijk deel daarvan uitmaakt;
Derde	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de Betrokkene, noch de Verwerkingsverantwoordelijke, noch de Verwerker, noch de personen die onder rechtstreeks gezag van de Verwerkingsverantwoordelijke of de Verwerker gemachtigd zijn om de Persoonsgegevens te Verwerken (artikel 4 sub 10 AVG);
Diensten	alle diensten die Partijen aan elkaar verlenen, zoals omschreven in de Overeenkomst;
EER	Europese Economische Ruimte, bestaande uit alle landen van de Europese Unie, Liechtenstein, Noorwegen en IJsland;
Overeenkomst	de overeenkomst zoals gespecificeerd in overweging A; Persoonsgegevens alle Persoonsgegevens die Verwerker ontvangt van of Verwerkt voor Verwerkingsverantwoordelijke in het kader van de uitvoering van de Overeenkomst (artikel 4 sub 1 AVG);
Sub-Verwerker	iedere niet-ondergeschikte Derde partij die door Verwerker is ingeschakeld bij de Verwerking van Persoonsgegevens. Dit gaat niet om Personeel;
UAVG	de Uitvoeringswet Algemene Verordening Gegevensbescherming. De UAVG heeft tot doel om uitvoering te geven aan de AVG;

Verwerker	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens Verwerkt (artikel 4 sub 8 AVG); Verwerkersovereenkomst de onderhavige overeenkomst met de daarbij horende Bijlagen;
Verstrekken	Het bekend maken of ter beschikking stellen van Persoonsgegevens;
Verwerking / Verwerken	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);
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 (artikel 4 sub 7 AVG);
Wbp	de Wet bescherming persoonsgegevens, wet van 6 juli 2000, houdende regels inzake de bescherming van Persoonsgegevens.

1.2 Alle definities in het enkelvoud hebben dezelfde betekenis als in het meervoud en vice versa.

1.3 Alle definities die vervoegingen zijn van gedefinieerde werkwoorden hebben dezelfde betekenis als de onvervoegde definities.

2 Algemeen

2.1. Deze Verwerkersovereenkomst betreft de hierboven beschreven Diensten die Verwerker levert aan Verwerkingsverantwoordelijke. De bepalingen uit onderhavige Verwerkersovereenkomst gaan voor op andere bepalingen met betrekking tot de Verwerking van Persoonsgegevens tussen Partijen, tenzij uitdrukkelijk schriftelijk anders overeengekomen.

2.2. Verwerker zal de Persoonsgegevens Verwerken in overeenstemming met de Overeenkomst en deze Verwerkersovereenkomst. Verwerkingsverantwoordelijke is ten aanzien van de Verwerking van Persoonsgegevens Verwerkingsverantwoordelijke. Verwerker is Verwerker.

2.3. Verwerker en Verwerkingsverantwoordelijke verstrekken elkaar over en weer tijdig alle benodigde informatie om een goede naleving van de geldende privacywet- en regelgeving moge-lijk te maken.

3. Gebruik Persoonsgegevens

3.1 Een overzicht van de Betrokkenen, de categorieën Persoonsgegevens, het doel waarvoor de Persoons-gegevens worden Verwerkt, overeengekomen Verwerkingen van Persoonsgegevens buiten de EER en Verwerkers, is opgenomen in Bijlage 1. Verwerker zal de Persoonsgegevens niet voor andere doeleinden of op andere wijze gebruiken dan voor het doel waarvoor de Persoonsgegevens zijn verstrekt of haar bekend zijn geworden.

3.2 Verwerker zal de Persoonsgegevens uitsluitend Verwerken in opdracht van Verwerkingsverantwoordelijke in het kader van de uitvoering van de Diensten en de Overeenkomst of in verband met een wettelijke verplichting.

3.3 Verwerker zal de Persoonsgegevens niet aan een Derde Verstrekken, tenzij deze uitwisseling plaatsvindt in het kader van de uitvoering van de Overeenkomst of Verwerkersovereenkomst of wanneer dit noodzakelijk is om te voldoen aan een wettelijke verplichting.

3.4 Indien Verwerkingsverantwoordelijke de Verwerker toestemming heeft verleend om Persoonsgegevens buiten de EER te Verwerken, ziet Verwerker er op toe dat de doorgifte van de Persoonsgegevens plaatsvindt in overeenstemming met de daarvoor geldende wettelijke voorschriften. Verwerker zal in Bijlage 1 opgave doen van de landen waar de gegevens worden Verwerkt en de maatregelen die Verwerker heeft getroffen om te voldoen aan de wettelijke voorschriften.

4. Geheimhouding

4.1 Verwerker houdt de Persoonsgegevens die zij Verwerkt in het kader van de uitvoering van de Overeenkomst geheim en zal alle nodige maatregelen treffen om geheimhouding van de Persoonsgegevens te verzekeren. Verwerker zal de verplichting tot geheimhouding tevens opleggen aan haar betrokken personeel en alle door haar ingeschakelde personen.

4.2 De in dit artikel bedoelde geheimhoudingsplicht geldt niet indien Verwerkingsverantwoordelijke uitdrukkelijk schriftelijk toestemming heeft gegeven om de Persoonsgegevens aan een Derde te Verstrekken, of een wettelijke verplichting bestaat om de Persoonsgegevens aan een Derde te Verstrekken.

5. Beveiliging Persoonsgegevens

5.1 Verwerker zal in overeenstemming met de geldende wet en regelgeving zodanige technische en organisatorische maatregelen treffen, in stand houden en zo nodig aanpassen, dat de Persoonsgegevens op passende wijze zijn beveiligd tegen verlies, onrechtmatige Verwerking of onrechtmatige toegang. Verwerker draagt er zorg voor dat de door haar gebruikte systemen (inclusief beveiligingssoftware en verbindingen) en de Diensten voldoen aan de geldende wettelijke verplichtingen in verband met de Verwerking van Persoonsgegevens.

5.2 Bij het vaststellen van de beveiligingsmaatregelen zal Verwerker rekening houden met de risico’s van de

Verwerking, de aard van de Persoonsgegevens en met name van de Verwerking van bijzondere Persoonsgegevens, zoals medische gegevens en de stand van de techniek.

5.3 In Bijlage 2 worden de afspraken tussen Partijen vastgelegd over de technische en organisatorische beveiligingsmaatregelen die Verwerker heeft getroffen. Deze maatregelen worden periodiek geëvalueerd en indien nodig aangepast.

6. Gegevensbeschermingseffectbeoordeling

6.1 Verwerker zal Verwerkingsverantwoordelijke in goed overleg voorzien van alle middelen, hulp en samenwerking waar Verwerkingsverantwoordelijke om vraagt om te voldoen aan diens verplichtingen betreffende een gegevensbeschermingseffectbeoordeling. Partijen zullen in goed overleg afspraken maken over de verdeling van de kosten die daarmee zijn gemoeid.

7. Controle

7.1 Verwerkingsverantwoordelijke heeft het recht om, maximaal één keer per jaar, met een aanzegging van twee weken, binnen reguliere kantoortijden, op eigen kosten door onafhankelijke deskundigen, een audit te laten uitvoeren inzake de Verwerking van Persoonsgegevens door Verwerker ter controle van deze Verwerkersovereenkomst. Verwerker zal alle redelijke medewerking verlenen aan een audit, waaronder het verlenen van toegang tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie. Indien Verwerker externe audits laat uitvoeren omtrent de beveiliging van Persoonsgegevens stuurt Verwerker zo spoedig mogelijk een kopie van de verklaring van de externe audit toe aan Verwerkingsverantwoordelijke.

7.2 Verwerker zal in overleg met Verwerkingsverantwoordelijke de aanbevelingen ter verbetering van de onafhankelijke deskundigen zo spoedig mogelijk uitvoeren.

7.3 In geval van een onderzoek door de AP, een andere bevoegde autoriteit of in geval enige (dreigende) procedure in verband met de Verwerking van Persoonsgegevens, zal Verwerker alle redelijke medewerking verlenen en Verwerkingsverantwoordelijke zo snel mogelijk informeren. Partijen zullen met elkaar in overleg treden over de wijze van optreden, alsmede over de maatregelen die getroffen moeten worden van de geldende privacywet- en regelgeving.

8. Beveiligingsincidenten

8.1 Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging indien zich Beveiligingsincident voordoet.

8.2 In geval van een Beveiligingsincident zal Verwerker onverwijld maatregelen treffen om de gevolgen van het incident en/of een nieuw incident te voorkomen. Verwerker zal alle medewerking verlenen aan Verwerkingsverantwoordelijke om aan haar meldplicht datalekken en het mogelijk informeren van Betrokkenen te kunnen voldoen.

8.3 Partijen leggen hun afspraken over de informatie-uitwisseling in verband met incidenten vast in Bijlage 3. Deze Bijlage kan ten allen tijde in overleg door Partijen worden gewijzigd. De Bijlage zal in ieder geval worden

aangepast indien de regelgeving meldplicht datalekken of de uitleg daarvan door de AP wijzigt.

8.4 In geval van een Beveiligingsincident dat leidt tot een meldplicht voor Verwerkingsverantwoordelijke, zal de melding in overleg met Verwerker door Verwerkingsverantwoordelijke worden verricht. Partijen zullen in goed overleg afspraken maken over de verdeling van de kosten die daarmee zijn gemoeid.

9. Verzoeken van Betrokkenen

9.1 Indien Verwerker een verzoek of klacht van een Betrokkene ontvangt, zoals een verzoek om informatie, inzage, rectificatie, gegevenswissing, verwerkingsbeperking, overdracht van de Persoonsgegevens, stuurt Verwerker dat verzoek zonder onredelijke vertraging door naar Verwerkingsverantwoordelijke.

9.2 Verwerker verleent Verwerkingsverantwoordelijke alle redelijke medewerking om ervoor te zorgen dat Verwerkingsverantwoordelijke binnen de wettelijke of contractuele termijnen kan voldoen aan de verplichtingen op grond van haar overeenkomsten, dan wel de geldende wet- en regelgeving. De redelijke kosten voor deze medewerking zullen door Verwerkingsverantwoordelijke aan Verwerker worden vergoed.

10. Sub-Verwerkers

10.1 Verwerker heeft bij de Verwerking van de Persoonsgegevens de mogelijkheid om met toestemming van Verwerkingsverantwoordelijke Sub-Verwerkers in te schakelen. Verwerkingsverantwoordelijke zal een redelijk verzoek om toestemming niet onthouden. In Bijlage 1 nemen Partijen de relevante gegevens over de Sub-Verwerkers op.

10.2 Verwerker zal met de door haar ingeschakelde Sub-Verwerkers een overeenkomst sluiten die in overeenstemming is met de relevante wet- en regelgeving en deze Verwerkersovereenkomst.

11. Toegang tot de Persoonsgegevens

11.1 De Persoonsgegevens behoren toe aan Verwerkingsverantwoordelijke. Op verzoek van Verwerkingsverantwoordelijke zal Verwerker de Persoonsgegevens in een gangbaar formaat ter beschikking stellen aan Verwerkingsverantwoordelijke.

12. Aansprakelijkheid en vrijwaring

12.1 Indien een Partij toerekenbaar tekortschiet in de nakoming van de Verwerkersovereenkomst is deze Partij aansprakelijk voor de schade en kosten die de andere Partij daardoor lijdt of heeft geleden. Partijen zijn uitsluitend aansprakelijk voor directe schade en in geen geval voor gevolgschade, zoals reputatieschade, bedrijfsschade of inkomsten- of winstderving. De hoogte van de door tekortgeschoten Partij te betalen schadevergoeding zal nooit hoger zijn dan het door de verzekering uit te betalen bedrag voor het relevante schadegeval, dan wel maximaal het door Verwerkingsverantwoordelijke betaalde bedrag aan Verwerker voor de dienstverlening over een periode van één jaar.

12.2 De in het vorige lid bedoelde uitsluitingen en beperkingen komen te vervallen indien en voor zover de schade het gevolg is van opzet of bewuste roekeloosheid van de bedrijfsleiding van de tekortgeschoten Partij.

12.3 Verwerker vrijwaart Verwerkingsverantwoordelijke voor boetes en/of dwangsommen van of namens de AP en/of andere bevoegde autoriteiten die aan Verwerkingsverantwoordelijke worden opgelegd en waarbij vast is komen te staan dat deze zijn toe te schrijven aan overtredingen van de Wbp of (U)AVG of Telecommunicatiewet door Verwerker. De in het eerste lid van dit artikel bedoelde uitsluitingen en beperkingen zijn hierop niet van toepassing. Om een beroep te kunnen doen op deze vrijwaring is Verwerkingsverantwoordelijke gehouden om:
(i) Verwerker terstond op de hoogte te brengen van enig onderzoek of andere aanleiding die zou kunnen leiden tot een voornemen van een toezichthouder tot het opleggen van een boete of last onder dwangsom;
(ii) in samenspraak met Verwerker te handelen en te communiceren richting de autoriteit;
en
(iii) tegen opgelegde boetes in bezwaar en/of beroep te gaan indien daar redelijkerwijs aanleiding voor is.

12.4 Verwerkingsverantwoordelijke vrijwaart Verwerker voor boetes en/of dwangsommen van of namens de AP en/of andere bevoegde autoriteiten die aan Verwerker worden opgelegd en waarbij vast is komen te staan dat deze zijn toe te schrijven aan overtredingen van de Wbp of (U)AVG of Telecommunicatiewet door Verwerkingsverantwoordelijke. De in het eerste lid van dit artikel bedoelde uitsluitingen en beperkingen zijn hierop niet van toepassing. Om een beroep te kunnen doen op deze vrijwaring is Verwerker gehouden om:
(i) Verwerkingsverantwoordelijke terstond op de hoogte te brengen van enig onderzoek of andere aanleiding die zou kunnen leiden tot een voornemen van een toezichthouder tot het opleggen van een boete of last onder dwangsom;
(ii) in samenspraak met Verwerkingsverantwoordelijke te handelen en te communiceren richting de autoriteit;
en
(iii) tegen opgelegde boetes in bezwaar en/of beroep te gaan indien daar redelijkerwijs aanleiding voor is.

13. Duur en beëindiging

13.1 Deze Verwerkersovereenkomst treedt in werking op de datum van ondertekening en eindigt van rechtswege bij beëindiging van de Overeenkomst of de Diensten.

13.2 Verwerker zal bij beëindiging van de Overeenkomst op verzoek van Verwerkingsverantwoordelijke en tegen vergoeding van de redelijke kosten de Persoonsgegevens ter beschikking stellen aan Verwerkingsverantwoordelijke of aan een door Verwerkingsverantwoordelijke aangewezen Derde.

13.3 Verwerker draagt er zorg voor dat zij zelf en de door haar ingeschakelde Sub-Verwerkers na beëindiging van de Verwerkersovereenkomst en na de volledige overdracht van de Persoonsgegevens (indien verzocht) de nog aanwezige Persoonsgegevens per direct zullen vernietigen onder overlegging van een vernietigingsrapport, tenzij een langere bewaring wettelijk verplicht is.

13.4 De afspraken die bestemd zijn om in stand te blijven na beëindiging van de Verwerkersovereenkomst zullen tussen Partijen blijven gelden. Dat geldt in ieder geval voor de geheimhoudingsplicht.

14. Wijziging Verwerkersovereenkomst

14.1 In geval van wijzigingen in de Diensten of regelgeving die van invloed zijn op de Verwerking van de

Persoonsgegevens zullen Partijen in overleg treden over de eventueel benodigde wijziging van de Verwerkersovereenkomst. De wijzigingen in de tekst van deze Verwerkersovereenkomst kunnen uitsluitend schriftelijk door de bevoegde vertegenwoordigers van Partijen worden overeengekomen.

14.2 Wijzigingen in de Bijlagen kunnen door Partijen op ieder moment schriftelijk worden gedaan onder vermelding van het versienummer en de datum van ingang van de nieuwe versie met een paraaf van de in Bijlage 1 genoemde contactpersonen.

15. Toepasselijk recht / Bevoegde rechter

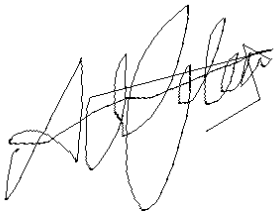
15.1 Op de Verwerkersovereenkomst is uitsluitend Nederlands recht van toepassing.

15.2 Alle geschillen die ontstaan naar aanleiding van deze Verwerkersovereenkomst worden beslecht op de wijze zoals opgenomen in de Overeenkomst.

ALDUS OVEREENGEKOMEN EN IN TWEEVOUD GETEKEND DOOR DE BEVOEGDE VERTEGENWOORDIGERS VAN PARTIJEN

Namens Verwerkingsverantwoordelijke

Naam: A Zengin Smit
Datum: 2018-10-04 15:50:47



Namens Verwerker

Naam: E. Kolks
Datum: 2018-10-04 15:50:47

BIJLAGE 1

A. Categorieën van Betrokkenen

De personen waarop de Persoonsgegevens betrekking hebben zijn in ieder geval:
Klanten (uw gegevens t.b.v. het uitvoeren en leveren van de diensten)
Eindgebruikers (in het geval u diensten registreert voor uw klanten of voor gebruik in uw eigen webapplicatie).

B. Soort Persoonsgegevens

De Persoonsgegevens die door Verwerker worden Verwerkt zijn in ieder geval:
NAW-gegevens;
Financiële gegevens;
Inloggegevens;
Inhoud van e-mails, contactformulieren en andere communicatie;

C. Bewaartermijnen

De Persoonsgegevens die door Verwerker worden Verwerkt mogen niet langer worden bewaard dan:
3 maanden na beëindiging van de Overeenkomst;

D. Aard en doel van de Verwerking

De Persoonsgegevens worden in ieder geval voor de volgende doeleinden Verwerkt
Hosting;
Beveiliging;
Opzetten netwerk;
Registratie WHOIS-database;
Facturatie.

F. Verwerking buiten de EER

Bij een domeinregistratie buiten de EER worden Persoonsgegevens buiten de EER Verwerkt. De vereiste Persoonsgegevens voor het registreren van het desbetreffende domein worden in dit geval verstrekt aan de desbetreffende/relevante WHOIS-domeindatabase(s).

G. Gegevens Sub-Verwerkers

Verwerker maakt voor de Diensten gebruik van de volgende Sub-Verwerkers:
Superior BV. (datacenterpartner welke ook de internetverbinding verzorgt).
De servers zijn allemaal gelokaliseerd in Helmond, NL

H. Diensten

Verwerker levert de volgende Diensten aan Verwerkingsverantwoordelijke:
• Webhosting
• Domeinregistratie
• E-mail
• SSL Certificaten

Versie
1.00A 25 mei 2018

BIJLAGE 2

Omschrijving van de technische en organisatorische beveiligingsmaatregelen die door de Verwerker zijn geïmplementeerd

- Logische toegangscontrole, gebruikmakend van sterke wachtwoorden;
- Automatische logging van alle handelingen rondom Persoongegevens;
- Fysieke maatregelen voor toegangsbeveiliging;
- Versleutelde opslag van digitale bestanden met Persoongegevens;
- Controle en toezicht op genomen beveiligingsmaatregelen;
- Organisatorische maatregelen voor toegangsbeveiliging;
- Steekproeven ter controle op de naleving van het beveiligingsbeleid;
- Doelgebonden toegangsbeperkingen;
- Controle op toegekende bevoegdheden

BIJLAGE 3: Meldplicht datalekkenprocedure

Wat is een Beveiligingsincident?

Een Beveiligingsincident is een inbreuk op de beveiliging 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, 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 AP:
- 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, stelt u zichzelf 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 (identiteit)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 u twijfelt, neem het zekere voor het onzekere en neem altijd contact op met WebReus (privacy@webreus.nl)

Waar meldt u het Beveiligingsincident?

Als u een Beveiligingsincident hebt ontdekt, neemt u direct contact op met WebReus:

E-mail: privacy@webreus.nl

Geef in uw e-mailbericht 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 AP moet worden verstrekt.

Gaarne de vragen zo volledig mogelijk en schriftelijk beantwoorden.

1. Geef een samenvatting van het Beveiligingsincident: 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. Omschrijf de groep personen waarop de Persoonsgegevens betrekking hebben.
Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van een kwetsbare groepen personen, zoals kinderen.

5. Is er sprake van één van deze specifieke groepen personen:
Ouderen JA / NEE
Kinderen JA / NEE
Zieken of mensen met een verstandelijke beperking: JA / NEE

6. Zijn de contactgegevens van de betrokken personen bekend?
Het kan zijn dat Betrokkenen geïnformeerd moeten worden over het Beveiligingsincident, kunnen we deze personen in dat geval bereiken?

7. Wat is de oorzaak (root cause) van het Beveiligingsincident?
Heeft u een idee hoe het Beveiligingsincident heeft kunnen ontstaan?

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

9. Wanneer is het Beveiligingsincident ontdekt?

10. Wat is de aard van de inbreuk?
Kan een onbevoegde de gegevens hebben ingezien JA / NEE
Kunnen de Persoonsgegevens zijn gekopieerd door een onbevoegde JA / NEE
Kunnen de Persoonsgegevens zijn gewijzigd (zoals hack in het systeem) JA / NEE
Kunnen de Persoonsgegevens zijn verwijderd (zoals ransomware) JA / NEE
Kunnen de Persoonsgegevens zijn gestolen JA / NEE

11. Om welke type Persoonsgegevens gaat het?
Naam-, adres- en woonplaatsgegevens JA / NEE
Telefoonnummer JA / NEE
E-mailadres of andere adres voor elektronische communicatie JA / NEE
Inloggegevens JA / NEE
Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer) JA / NEE
Burgerservicenummer (BSN) JA / NEE
Paspoortkopieën of kopieën van andere legitimatiebewijzen JA / NEE
Geslacht JA / NEE
Geboortedatum en/of leeftijd JA / NEE
(Pas)foto JA / NEE
Geboorteland JA / NEE
Medische gegevens (waaronder ook medicijnen of medische hulpmiddelen) JA / NEE
Biometrische gegevens (bijv. vingerafdruk, DNA) JA / NEE
Gegevens over schulden/kredieten JA / NEE
Inkomensgegevens JA / NEE
Gegevens over iemands betalingsverkeer JA / NEE
Gegevens over wettelijke vertegenwoordiging (bewindvoerder/mentor) JA / NEE
Verslavingsgegevens JA / NEE
School/werkprestaties JA / NEE
Gegevens over relationele problemen JA / NEE
Gegevens over (vermoeden van) mishandeling JA / NEE
Religie JA / NEE
Strafrechtelijke gegevens (ook bijv. straatverboden) JA / NEE
Politieke overtuiging JA / NEE

Vakbondslidmaatschap JA / NEE
Seksuele voorkeur / geaardheid JA / NEE

12. Welke gevolgen kan de inbreuk hebben voor de getroffen personen?

Stigmatisering of uitsluiting JA / NEE
Schade aan de gezondheid JA / NEE
Kans op identiteitsfraude JA / NEE
Kans op financiële schade (bijv. fraude met creditcardgegevens) JA / NEE
Blootstelling aan spam of phishing JA / NEE
Andere gevolgen, namelijk:

13. Omschrijf welke technische en organisatorische maatregelen zijn getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

14. Zijn de gelekte Persoonsgegevens beveiligd?

Zijn de Persoonsgegevens versleuteld JA / NEE
Zo ja, welke versleuteling? _____
Zo ja, voor welke Persoonsgegevens? _____

Zijn de Persoonsgegevens gehasht? JA / NEE
Zo ja, op welke wijze? _____

Kunnen de Persoonsgegevens vanaf afstand worden gewist JA / NEE
Zo ja, is dat gebeurd en wanneer?_____

Zijn de Persoonsgegevens op een andere manier ontoegankelijk gemaakt? JA / NEE
Zo ja, hoe en wanneer is dat gebeurd?_____

15. Zijn er Persoonsgegevens van personen in andere EU-landen getroffen door het Beveiligingsincident? Zo ja, welke uit welke landen?