Helperpark 278-D
9723 ZA Groningen

050 211 24 88
info@squidmedia.nl

WWW.SQUIDMEDIA.NL

kvk 02064778
btw NL108730384B01
iban NL22 RABO 0320 7049 39

SQUID MEDIA

VERWERKERSOVEREENKOMST

DOCUMENT TYPE	VERWERKERSOVEREENKOMST
GESCHREVEN VOOR	SQUID Media
DATUM	13-9-2018
STATUS	DEFINITIEF
VERSIE	1.0

ontwerpen maken beheren verbeteren

PARTIJEN

Deze Verwerkersovereenkomst is van toepassing op alle vormen van Verwerking van Persoonsgegevens die SQUID Media, ingeschreven bij de Kamer van Koophandel onder nummer 02064778, (hierna: Verwerker) uitvoert ten behoeve van een wederpartij aan wie zij diensten levert (hierna: Verwerkings-verantwoordelijke). Verwerkingsverantwoordelijke en Verwerker worden hieronder gezamenlijk aangeduid als Partijen.

ARTIKEL 1. DEFINITIES

In deze Verwerkersovereenkomst wordt verstaan onder:

1. Persoonsgegeven: Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
2. Verwerken of Verwerking: 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 ter beschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
3. Datalek: een inbreuk op de beveiliging van Persoonsgegevens die per ongeluk of op onrechtmatige wijze leidt tot - of waarbij redelijkerwijs niet uit te sluiten valt dat die kan leiden tot - de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte Persoonsgegevens, en die waarschijnlijk een risico inhoudt voor de rechten en vrijheden van Betrokkene(n);
4. Betrokkene: degene op wie een Persoonsgegeven betrekking heeft;
5. AP: de Autoriteit Persoonsgegevens, het zelfstandig bestuursorgaan dat in Nederland bij wet als toezichthouder is aangesteld voor het toezicht op de Verwerking van Persoonsgegevens;
6. AVG: de Algemene Verordening Gegevensbescherming;
7. Verwerkersovereenkomst: deze verwerkersovereenkomst.
8. Onderaannemer / subverwerker Datacenter: de hostingpartij die als subverwerker van Verwerker de dienstverlening met betrekking tot webhosting voor Verwerkingsverantwoordelijke verzorgt.

ARTIKEL 2. TOEPASSINGSBEREIK VERWERKERSOVEREENKOMST

2.1. Deze Verwerkersovereenkomst is van toepassing op de Verwerking van Persoonsgegevens door Verwerker ten behoeve van Verwerkingsverantwoordelijke die plaatsvindt in het kader van de dienstverlening van Verwerker aan Verwerkingsverantwoordelijke, zoals nader geregeld in de tussen Partijen gesloten overeenkomst van dienstverlening en/of de Algemene Voorwaarden van SQUID Media.

2.2. Er is onder meer sprake van Verwerking van Persoonsgegevens door Verwerker ten behoeve van Verwerkingsverantwoordelijke in de zin van het voorgaande artikellid, voor zover Verantwoordelijke in het kader van haar gebruik van de dienstverlening van Verwerker Persoonsgegevens opslaat in de 'cloud'. Partijen bevestigen dat Verwerkingsverantwoordelijke in dat geval volledig verantwoordelijk is voor het vaststellen van het doel en de middelen voor de verwerking van Persoonsgegevens. Het zal Verwerker veelal onbekend zijn welke Persoonsgegevens bij haar worden opgeslagen door Verwerkingsverantwoordelijke, en voor welke doeleinden dat gebeurt, en zij kan haar dienstverlening daar niet op afstemmen. Het is dus aan de Verantwoordelijke om te bepalen dat zij de Persoonsgegevens onder de overeengekomen voorwaarden bij Verwerker mag opslaan.

2.3. Partijen erkennen dat Verwerker ook Persoonsgegevens Verwerkt in het kader van de dienstverlening waarvoor zij zelf het doel en de middelen bepaalt. Dit geldt bijvoorbeeld voor Persoonsgegevens over contactpersonen bij de Verwerkingsverantwoordelijke. Op de Verwerking van deze Persoonsgegevens, die aan de AVG moet voldoen, is deze Verwerkersovereenkomst niet van toepassing.

2.4. De Verwerking van Persoonsgegevens onder deze Verwerkersovereenkomst heeft niet tot gevolg dat Verwerkingsverantwoordelijke enige intellectuele eigendomsrechten of andere aanspraken op de Persoonsgegevens overdraagt aan Verwerker, en is evenmin bedoeld om op enigerlei wijze afbreuk te doen aan de rechten van Betrokkenen.

ARTIKEL 3. VERPLICHTINGEN VERWERKER

3.1. Verwerker zal de Persoonsgegevens uitsluitend ten behoeve van de Verwerkingsverantwoordelijke Verwerken, en slechts voor zover noodzakelijk voor de dienstverlening van Verwerker aan Verwerkingsverantwoordelijke, alsmede voor die doeleinden die daarmee redelijkerwijs samenhangen of die tussen Partijen nader schriftelijk worden bepaald. Verwerker zal de Persoonsgegevens niet voor enig ander doel verwerken dan zoals door Verwerkingsverantwoordelijke is vastgesteld.

3.2. De Verwerker zal de Verwerkingsverantwoordelijke onmiddellijk in kennis stellen indien naar zijn mening een instructie van de Verwerkingsverantwoordelijke in strijd is met de AVG of andere relevante wet- en regelgeving.

3.3. Verwerker zal ervoor zorgen dat haar verplichtingen uit deze Verwerkersovereenkomst worden opgelegd aan degenen die Persoonsgegevens verwerken onder het gezag van Verwerker, waaronder begrepen maar niet beperkt tot werknemers.

3.4. Verwerker zal, voor zover dat binnen haar macht ligt, bijstand verlenen aan Verwerkings-verantwoordelijke in het nakomen van zijn verplichtingen:

i. om verzoeken te beantwoorden van Betrokkenen die hun rechten uitoefenen onder de AVG;
ii. met betrekking tot de beveiliging van de Verwerking van de Persoonsgegevens, de melding van Datalekken aan de AP en de Betrokkenen;
iii. een mogelijk vereiste gegevensbeschermingseffectbeoordeling ('Privacy Impact Assessment') en voorafgaande raadpleging van de AP.

Eventuele kosten verbonden aan deze bijstand zijn niet in de overeengekomen prijzen en vergoedingen van Verwerker begrepen. Verwerker is gerechtigd redelijke kosten voor het verlenen van deze bijstand aan Verwerkingsverantwoordelijke door te belasten. Indien sprake is van dergelijke kosten, zal Verwerker dit zo mogelijk tevoren aangeven.

3.5. In het geval dat een Betrokkene een verzoek tot uitoefening van zijn/haar wettelijke rechten richt aan Verwerker, zal Verwerker het verzoek doorsturen aan Verwerkingsverantwoordelijke, en zal Verwerkingsverantwoordelijke het verzoek verder afhandelen, onverminderd het bepaalde in artikel 3.4.i. Verwerker mag de betrokkene daarvan op de hoogte stellen.

ARTIKEL 4. VERPLICHTINGEN VERANTWOORDELIJKE

4.1. Verwerkingsverantwoordelijke zal Verwerker op de hoogte stellen van de identiteit van haar functionaris voor de gegevensbescherming en/of vertegenwoordiger, voor zover zij die heeft aangesteld. Wijzigingen dienen onverwijld te worden doorgegeven aan Verwerker. Indien Verwerkingsverantwoordelijke geen functionaris of vertegenwoordiger opgeeft, zal Verwerker ervan uitgaan dat Verwerkingsverantwoordelijke die niet heeft aangesteld.

4.2. Verwerkingsverantwoordelijke garandeert dat de inhoud, het gebruik van en de opdracht tot de Verwerkingen van de Persoonsgegevens zoals bedoeld in deze Verwerkersovereenkomst niet onrechtmatig zijn en geen inbreuk maken op enig recht van derden.

ARTIKEL 5. INSCHAKELEN VAN ONDERAANNEMERS

5.1. Verwerker mag in het kader van deze Verwerkersovereenkomst gebruik maken van derden. Een actuele lijst van onderaannemers die door Verwerker worden ingeschakeld bij de Verwerking van Persoonsgegevens onder deze Overeenkomst is beschikbaar en kan schriftelijk worden opgevraagd bij Verwerker.

5.2. Verwerker zal ervoor zorgen dat onderaannemers schriftelijk ten minste dezelfde plichten op zich nemen jegens Verwerker als tussen Verwerkingsverantwoordelijke en Verwerker zijn overeengekomen in deze Verwerkersovereenkomst. Verwerker staat jegens

Verwerkingsverantwoordelijke in voor een correcte naleving van deze plichten door haar onderaannemers.

ARTIKEL 6. DOORGIFTE VAN PERSOONSGEGEVENS

6.1. Verwerker mag de persoonsgegevens verwerken in landen binnen de Europees Economische Ruimte (EER). Doorgifte naar landen buiten de EER is zonder toestemming van de Verwerkingsverantwoordelijke verboden.

ARTIKEL 7. BEVEILIGING

7.1. Verwerker en subverwerker Datacenter zullen, rekening houdend met de stand van de techniek, de uitvoeringskosten en de haar bekende informatie over de verwerkingsdoeleinden en de risico's van de Verwerking, passende technische en organisatorische maatregelen nemen met betrekking tot de te verrichten Verwerkingen van Persoonsgegevens, tegen verlies of tegen enige vorm van onrechtmatige Verwerking (zoals onbevoegde toegang tot of ongeoorloofde aantasting, wijziging of verstrekking van de Persoonsgegevens).

7.2. Verwerker en subverwerker Datacenter hebben in ieder geval de maatregelen genomen zoals genoemd in het Beveiligingsprotocol, waarvan de actuele versie is aangehecht in respectievelijk Bijlage A en B. Onverminderd haar verplichting uit hoofde van het voorgaande artikellid, mogen Verwerker en subverwerker Datacenter het Beveiligingsprotocol op ieder moment eenzijdig aanpassen. De actuele versie van het Beveiligingsprotocol kan bij Verwerker schriftelijk worden opgevraagd. Verwerkingsverantwoordelijke zal ten aanzien van het Beveiligingsprotocol geheimhouding betrachten conform Artikel 9.

7.3. Verwerker en subverwerker Datacenter werken conform standaarden die geacht worden te voldoen aan de beveiligingseisen rekening houdend met de stand van de techniek. Deze standaarden zijn nader beschreven in respectievelijk Bijlage A en B.

7.4. Subverwerker Datacenter zorgt ervoor dat periodiek (en tenminste jaarlijks) een audit rapport wordt opgesteld door een gekwalificeerde derde partij, waarin deze haar oordeel geeft over de door subverwerker Datacenter getroffen beveiligingsmaatregelen in het licht van deze Verwerkersovereenkomst, en de door subverwerker Datacenter toegepaste standaarden. Dit audit rapport wordt op verzoek kosteloos aan Verwerkingsverantwoordelijke beschikbaar gesteld, teneinde de Verwerkingsverantwoordelijke in staat te stellen om de naleving van dit artikel objectief vast te stellen.

ARTIKEL 8. MELDPLICHT

8.1. Verwerkingsverantwoordelijke is te allen tijde verantwoordelijk voor de wettelijk vereiste melding van een Datalek aan de AP en/of Betrokkenen.

8.2. Om Verwerkingsverantwoordelijke in staat te stellen aan deze wettelijke plicht te voldoen, stelt Verwerker de Verwerkingsverantwoordelijke onverwijld en indien mogelijk binnen 24 uur nadat is vastgesteld dat sprake is van een Datalek, op de hoogte van een eventueel Datalek. Melding wordt gedaan aan de aan ons bekende contactgegevens, dan wel de tussen partijen gangbare communicatie kanalen.

8.3. De mededeling door de Verwerker maakt in elk geval melding van het feit dat er een Datalek is geweest. Daarnaast beschrijft de mededeling:

- de aard van het Datalek, waar mogelijk onder vermelding van de categorieën van Betrokkenen en, bij benadering, de duur en omvang van het Datalek;
- de naam en de contactgegevens van de functionaris voor gegevensbescherming van Verwerker of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van het Datalek;
- de maatregelen die de Verwerker heeft voorgesteld of genomen om het Datalek aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

ARTIKEL 9. GEHEIMHOUDING EN VERTROUWELIJKHEID

9.1. Op alle Persoonsgegevens die Verwerker van Verwerkingsverantwoordelijke ontvangt en/of zelf verzamelt in het kader van deze Verwerkersovereenkomst, rust een geheimhoudingsplicht jegens derden. Verwerker zal deze informatie niet voor een ander doel gebruiken dan waarvoor zij deze heeft verkregen.

9.2. Deze geheimhoudingsplicht is niet van toepassing voor zover Verwerkingsverantwoordelijke uitdrukkelijke toestemming heeft gegeven om de informatie aan derden te verschaffen, indien het verstrekken van de informatie aan derden logischerwijs noodzakelijk is gezien de aard van de verstrekte opdracht en de uitvoering van deze Verwerkersovereenkomst, of indien er een wettelijke verplichting bestaat om de informatie aan een derde te verstrekken.

9.3. Indien Verwerker op grond van een wettelijke verplichting gehouden is om Persoonsgegevens aan een derde te verstrekken, zal zij Verwerkingsverantwoordelijke hiervan tevoren op de hoogte stellen, tenzij dit verboden is onder de betreffende wetgeving.

ARTIKEL 10. AUDIT

10.1. Verwerkingsverantwoordelijke heeft het recht om het in Artikel 7.4 genoemde audit rapport op te vragen. Indien het in het kader van haar verantwoordingsplicht voor Verwerkingsverantwoordelijke redelijkerwijs noodzakelijk is om, in aanvulling op dit audit rapport, nadere zekerheden te verkrijgen dan zal Verwerker dit faciliteren en zullen Partijen in overleg treden over de nadere invulling en uitwerking daarvan. Verwerker is gerechtigd alle daaraan verbonden kosten in rekening te brengen bij Verwerkingsverantwoordelijke.

10.2. Verwerkingsverantwoordelijke heeft het recht om audits uit te laten voeren op de naleving van deze Verwerkersovereenkomst indien dit gebeurt door of namens een wettelijke toezichthouder (“right to examine/right to audit”) op grond van een wettelijke bevoegdheid tot controle van naleving van de AVG of andere op Verwerkingsverantwoordelijke toepasselijke wet- en regelgeving. Op verzoek van Verwerker toont Verwerkingsverantwoordelijke aan dat sprake is van een dergelijke wettelijke bevoegdheid.

10.3. Verwerker zal aan de in het vorige artikellid genoemde audit meewerken en alle voor de audit redelijkerwijs relevante gegevens en medewerkers tijdig ter beschikking stellen.

10.4. De bevindingen naar aanleiding van de uitgevoerde audit zullen aan Verwerker beschikbaar worden gesteld en door Verwerker worden beoordeeld en kunnen, naar eigen goeddunken van Verwerker en op de wijze zoals Verwerker zelf bepaalt, worden doorgevoerd door Verwerker.

10.5. Alle kosten in verband met de audit worden door Verwerkingsverantwoordelijke gedragen. Eventuele kosten verbonden aan de medewerking door Verwerker zijn niet in de overeengekomen prijzen en vergoedingen van Verwerker begrepen. Verwerker is gerechtigd redelijke kosten voor het verlenen van deze bijstand aan Verwerkingsverantwoordelijke door te belasten. Indien sprake is van dergelijke kosten, zal Verwerker dit zo mogelijk tevoren aangeven.

ARTIKEL 11. AANSPRAKELIJKHEID

11.1. De aansprakelijkheid van Verwerker jegens Verwerkingsverantwoordelijke voor schade (waaronder schade als gevolg van eventuele aanspraken van de AP en/of Betrokkenen, en alle daarmee verband houdende kosten) als gevolg van een toerekenbare tekortkoming door Verwerker in de nakoming van zijn verplichtingen onder deze Verwerkersovereenkomst, de AVG, dan wel uit onrechtmatige daad of anderszins, is per gebeurtenis (waarbij een reeks van opeenvolgende gebeurtenissen geldt als één gebeurtenis) beperkt in de zin van Artikel 15 van de Algemene Voorwaarden van SQUID Media.

11.2. Verwerkingsverantwoordelijke vrijwaart Verwerker voor schade (waaronder schade als gevolg van eventuele aanspraken van de AP en/of Betrokkenen, en alle daarmee verband houdende kosten),

indien deze aanspraak een toerekenbare tekortkoming betreft van Verwerkingsverantwoordelijke van zijn verplichtingen onder deze Verwerkersovereenkomst of de AVG.

ARTIKEL 12. DUUR EN BEËINDIGING

12.1. Deze Verwerkersovereenkomst komt tot stand ofwel door ondertekening van Partijen en op de datum van de laatste ondertekening, ofwel door actieve en ondubbelzinnige toestemming via de website van Verwerker en op de datum dat deze toestemming gegeven is.

12.2. Deze Verwerkersovereenkomst is aangegaan voor de duur zoals bepaald in de hoofdovereenkomst tussen Partijen en bij gebreke daarvan in ieder geval voor de duur van de samenwerking, dat wil zeggen: zo lang als Verwerkingsverantwoordelijke gebruik maakt van dienstverlening van Verwerker waarbij Verwerker ten behoeve van Verwerkingsverantwoordelijke Persoonsgegevens Verwerkt.

12.3. Bij beëindiging van de Verwerkersovereenkomst, om welke reden en op welke wijze dan ook, zal Verwerker Verwerkingsverantwoordelijke 2 maanden gelegenheid bieden om een elektronische kopie op te vragen van alle persoonsgegevens die bij haar aanwezig zijn, en zal zij aansluitend, maar uiterlijk binnen 3 maanden na het einde van de Verwerkersovereenkomst, eventuele resterende kopieën daarvan wissen, tenzij Verwerker wettelijk verplicht is de gegevens te bewaren.

ARTIKEL 13. OVERIGE BEPALINGEN

13.1. Deze Verwerkersovereenkomst verwoordt de enige geldende afspraken tussen Verwerkings-verantwoordelijke en Verwerker betreffende de verwerking van Persoonsgegevens door Verwerker en vervangt alle voorgaande bewerkersovereenkomsten en andere schriftelijke dan wel mondelinge afspraken en correspondentie over dat onderwerp.

13.2. Ingeval van strijdigheid van de bepalingen van deze Verwerkersovereenkomst met de Algemene Voorwaarden van SQUID Media, prevaleert deze Verwerkersovereenkomst.

13.3. Mededelingen betrekking hebbend op deze Verwerkersovereenkomst dienen schriftelijk te worden gedaan.

13.4. Deze Verwerkersovereenkomst is aangegaan met het doel te voldoen aan de vereisten gesteld door de AVG aan de Verwerking van Persoonsgegevens door Verwerker ten behoeve van Verwerkingsverantwoordelijke. Indien de wettelijke vereisten vergen dat deze Verwerkersovereenkomst wordt gewijzigd, mag elke Partij een wijzigingsvoorstel doen, waarna de Partijen in goed vertrouwen onderhandelingen zullen aangaan om overeenstemming te bereiken, om de voortdurende naleving van de toepasselijke wetgeving te verzekeren.

13.5. Verwerker is daarnaast gerechtigd deze Verwerkersovereenkomst van tijd tot tijd eenzijdig te herzien. Zij zal minimaal één maand van tevoren mededeling doen van de wijzigingen aan Verwerkingsverantwoordelijke. Verwerkingsverantwoordelijke mag opzeggen tegen het einde van deze maand indien zij niet akkoord kan gaan met de wijzigingen. Een akkoord met de gewijzigde voorwaarden kan elektronisch worden gegeven. Indien de Verwerkingsverantwoordelijke een maand na aankondiging van de gewijzigde voorwaarden gebruik maakt van de dienstverlening van Verwerker waarop de Verwerkersovereenkomst betrekking heeft, geldt dit ook als een akkoord met de gewijzigde voorwaarden.

ARTIKEL 14. TOEPASSELIJK RECHT EN GESCHILLENBESLECHTING

14.1. De Verwerkersovereenkomst en de uitvoering daarvan worden beheerst door Nederlands recht.

14.2. Alle geschillen, welke tussen Partijen mochten ontstaan in verband met de Verwerkersovereenkomst, zullen worden voorgelegd aan de bevoegde rechter voor het arrondissement waarin Verwerker gevestigd is.

BIJLAGE A. BEVEILIGINGSPROTOCOL VERWERKER

In deze Bijlage worden de technische en organisatorische maatregelen ter beveiliging van de Verwerking van Persoonsgegevens door Verwerker nader beschreven.

1. STANDAARDEN MET BETREKKING TOT INFORMATIEBEVEILIGING

Verwerker werkt in toenemende mate conform ISO 27001, welke standaarden geacht worden te voldoen aan de beveiligingseisen rekening houdend met de stand van de techniek.

2. TOEGANGSCONTROLE TOT BEDRIJFSTERREIN EN –GEBOUW (FYSIEK)

- Verwerker hanteert fysieke beveiliging voor haar kantoorlocatie. Ongeautoriseerde toegang wordt verhinderd.
- Fysieke toegang tot de kantoorlocatie is altijd onder begeleiding van één of meerdere medewerker(s) van Verwerker.

3. TOEGANGSCONTROLE TOT SYSTEMEN (DIGITAAL)

- Toegang wordt aan medewerkers verleend door middel van procedures voor toegangsverzoeken.
- Toegang tot (klant)systemen die persoonlijk identificeerbare informatie verwerken staat in relatie tot de taak die de medewerker vervult;

4. TOEGANGSCONTROLE TOT DE PERSOONSGEGEVENS

- Gebruikers worden, zodra zij zijn geauthentiseerd, uitsluitend geautoriseerd voor de toegangs-niveaus die bij hun functies horen;
- Verwerker zal per direct toegang van medewerkers of derden intrekken als gevolg van beëindiging van de arbeidsrelatie of het contract en na waarneming van inactiviteit van de gebruikers of langdurige afwezigheid.

5. MAATREGELEN TEN AANZIEN VAN PERSONEEL

- Relevant personeel is opgeleid om systemen en applicaties die worden ingezet voor de Verwerking van Persoonsgegevens op een adequate wijze in te richten en te beheren;
- Met alle medewerkers is schriftelijk geheimhouding overeengekomen als vast onderdeel van het arbeidscontract;
- Waar van toepassing is functiescheiding aangebracht om toegang tot ontwikkel, test en productieomgevingen te scheiden en alleen de juiste medewerkers toegang te verschaffen tot de juiste systemen en informatie.

6. MAATREGELEN TEN AANZIEN VAN BESCHIKBAARHEID

- Computers en laptops zijn beschermd door anti-malware oplossingen die met grote regelmaat updates ontvangen van nieuwe definities;
- Indien malware wordt ontdekt zal Verwerker direct stappen ondernemen om de verspreiding en mogelijke impact van de malware te minimaliseren door de dreiging uit te schakelen;

N.B. De in deze bijlage beschreven maatregelen bieden geen garantie of zekerheid dat elke vorm van ongeautoriseerde toegang, gebruik, of ongewenst verlies van persoonsgegevens zal worden voorkomen.

BIJLAGE A. BEVEILIGINGSPROTOCOL SUBVERWERKER DATACENTER

In deze Bijlage worden de technische en organisatorische maatregelen ter beveiliging van de Verwerking van Persoonsgegevens door subverwerker Datacenter nader beschreven.

1. STANDAARDEN MET BETREKKING TOT INFORMATIEBEVEILIGING

Datacenter werkt conform ISO 27001 en NEN 7510, welke standaarden geacht worden te voldoen aan de beveiligingseisen rekening houdend met de stand van de techniek.

2. TOEGANGSCONTROLE TOT BEDRIJFSTERREINEN EN –GEBOUWEN (FYSIEK)

- Datacenter hanteert fysieke beveiligingssystemen bij alle datacenterlocaties die worden gebruikt ten behoeve van de Verwerking;
- Fysieke toegangscontrole is geïmplementeerd voor alle datacenters. Ongeautoriseerde toegang wordt verhinderd met behulp van beveiligingspersoneel ter plaatse en de inzet van onder meer beveiligingscamera's (24 uur per dag, zeven dagen per week);
- Datacenter hanteert procedures voor het verstrekken van identificatiebadges om personeel te autoriseren en om fysieke toegang tot systemen te beheren;
- Toegangspoorten zijn met kaartlezers uitgerust en werknemers moeten een geldig identiteitsbewijs presenteren voordat zij een datacenterlocatie van Datacenter mogen betreden;
- Bezoekers moeten voordat zij een datacenter kunnen bezoeken goedkeuring hebben ontvangen van Datacenter medewerkers. Bezoekers dienen bij aanmelding identificatie te tonen, een gastenboek te tekenen en worden te allen tijde begeleid wanneer zij zich in het datacenter bevinden.

3. TOEGANGSCONTROLE TOT SYSTEMEN (DIGITAAL)

- Toegang wordt aan medewerkers verleend door middel van gedocumenteerde procedures voor toegangsverzoeken. Hun operationeel managers moeten deze verzoeken goedkeuren voordat de aanvullende toegang wordt verleend;
- Toegang tot (klant)systemen die persoonlijk identificeerbare informatie verwerken staat in relatie tot de taak die de medewerker vervult;
- Toegangscontrole is ingeschakeld op besturingssystemen, databases en applicaties;
- Aan iedere unieke eindgebruiker wordt een enkel account verstrekt zodat altijd traceerbaar en aantoonbaar is wie een specifieke handeling heeft uitgevoerd. Het is niet toegestaan om accounts te delen.

4. TOEGANGSCONTROLE TOT DE PERSOONSGEGEVENS

- Gebruikers worden, zodra zij zijn geauthentiseerd, uitsluitend geautoriseerd voor de toegangs-niveaus die bij hun functies horen;

- Datacenter zal per direct toegang van medewerkers of derden intrekken als gevolg van beëindiging van de arbeidsrelatie of het contract en na waarneming van inactiviteit van de gebruikers of langdurige afwezigheid.

5. INVOER CONTROLE

- Datacenter houdt logs bij met betrekking van toegang tot Persoonsgegevens die onder de beheerdersverantwoordelijkheid van Datacenter vallen. Deze logbestanden worden, waar mogelijk, op een gecentraliseerde locatie opgeslagen om ongeautoriseerde aanpassingen van derden tegen te gaan.
- De systemen van Datacenter zijn geconfigureerd om event logging bij te houden zodat een inbreuk op de beveiliging achteraf kan worden vastgesteld. Datacenter treft maatregelen om deze logbestanden te beschermen tegen ongeautoriseerde toegang of wijziging;
- Partijen zorgen ervoor dat invoer-controlemaatregelen worden toegepast op de eigen systemen en, waar relevant, die van haar klanten voor zover deze worden ingezet voor toegang tot en verwerking van Persoonsgegevens.

6. MAATREGELEN TEN AANZIEN VAN PERSONEEL

- Relevant personeel is opgeleid om systemen en applicaties die worden ingezet voor de Verwerking van Persoonsgegevens op een adequate wijze in te richten en te beheren;
- Met alle medewerkers is schriftelijk geheimhouding overeengekomen als vast onderdeel van het arbeidscontract;
- Waar van toepassing is functiescheiding aangebracht om toegang tot ontwikkel, test en productieomgevingen te scheiden en alleen de juiste medewerkers toegang te verschaffen tot de juiste systemen en informatie.

7. MAATREGELEN TEN AANZIEN VAN BESCHIKBAARHEID

- Computers en laptops zijn beschermd door anti-malware oplossingen die met grote regelmaat updates ontvangen van nieuwe definities;
- Indien malware wordt ontdekt zal Datacenter direct stappen ondernemen om de verspreiding en mogelijke impact van de malware te minimaliseren door de dreiging uit te schakelen;
- Beschikbaarheid van kritieke infrastructuurcomponenten die door Datacenter voor beheerdoeleinden worden ingezet is door de inzet van beschikbaarheidsmaatregelen als redundantie, high availability en geografische spreiding van datacentra geborgd;
- Door Datacenter is een Computer Emergency Response Team ingesteld dat optreedt bij eventuele informatiebeveiligingsincidenten. Dit team bestaat uit een medewerkers met verschillende specialisaties om zo adequaat optreden te borgen.

N.B. De in deze bijlage beschreven maatregelen bieden geen garantie of zekerheid dat elke vorm van ongeautoriseerde toegang, gebruik, of ongewenst verlies van persoonsgegevens zal worden voorkomen.