

- Concept - Verwerkersovereenkomst

Overeenkomst ter bescherming van persoonsgegevens

Gegenereerd op: 14-04-2022

Partijen:

1. **Eyetractive BV**, hierna te noemen "**Verwerker**", gevestigd te Stein aan Heerstraat-Centrum 131 (6171 HV), vertegenwoordigd door Jan Huntjens.
2. **Testklant**, hierna te noemen "**Verwerkingsverantwoordelijke**", gevestigd te **Heerstraat Centrum 131 6171 HV Stein**, vertegenwoordigd door Paul Testvogel.

Hierna gezamenlijk te noemen 'Partijen';

In aanmerking nemende dat:

1. Verwerkingsverantwoordelijke (diensten/producten) aanbiedt voor;
2. Verwerker dienstverlening aanbiedt in het kader van;
3. Partijen hebben een overeenkomst gesloten met betrekking tot Voorbeeldproject, ingaande op 01-01-2022, hierna te noemen: "Hoofdovereenkomst". In het kader van de uitvoering van de overeenkomst verleent verwerker diensten aan verwerkingsverantwoordelijke;
4. Verwerker in het kader van de uitvoering van de overeenkomst ook Persoonsgegevens verwerkt voor Verwerkingsverantwoordelijke;
5. Partijen verplicht zijn om op grond van de geldende privacy wet- en regelgeving afspraken te maken en vast te leggen met betrekking tot de verwerking van Persoonsgegevens door Verwerker;
6. De bepalingen van deze Verwerkersovereenkomst voor gaan op alle afspraken die tussen Partijen gelden en betrekking hebben op de verwerking van Persoonsgegevens door Verwerker voor Verwerkingsverantwoordelijke.

Komen als volgt overeen:

Definities / begrippen

1.1 AP: Autoriteit Persoonsgegevens, de toezichthoudende autoriteit voor de naleving van de geldende privacywetgeving.

1.2 Betrokkene: de natuurlijke persoon waarop de Persoonsgegevens die Verwerker verwerkt voor Verwerkingsverantwoordelijke en/of haar opdrachtgevers in het kader van de uitvoering van de Overeenkomst betrekking hebben.

1.3 Datalek: een inbreuk op de beveiliging van Persoonsgegevens die ernstige nadelige gevolgen heeft voor de bescherming van Persoonsgegevens.

1.4 Overeenkomst: de hoofdovereenkomst waar deze Verwerkersovereenkomst uit voortvloeit. Met als titel Voorbeeldproject, startdatum 01-01-2022 en einddatum onbepaald (nog lopend). Dit wordt verder gedefinieerd in artikel 3.

1.5 Personeel: de door Partijen voor de uitvoering van deze Verwerkersovereenkomst in te schakelen personen, welke onder hun verantwoordelijkheid zullen werken.

1.6 Persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Ook (herleidbare) gepseudonimiseerde persoonsgegevens vallen onder dit begrip.

1.7 Sub-Verwerker: derde die door Verwerker wordt ingeschakeld om ten behoeve van Verwerker Persoonsgegevens te verwerken, zonder aan het rechtstreeks gezag van Verwerker te zijn onderworpen.

1.8 Verwerkingsverantwoordelijke (ook wel Verantwoordelijke genoemd): de verantwoordelijke voor de Verwerking in de zin van de Europese verordeningen en richtlijnen ten aanzien van bescherming van persoonsgegevens (AVG).

1.9 Verwerker (ook wel Bewerker genoemd): (i.c. eyetractive) degene die ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt zonder aan zijn rechtstreeks gezag te zijn onderworpen.

1.10 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 terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegeven.

2. Algemeen

2.1 Verwerkingsverantwoordelijke wordt ten aanzien van de Persoonsgegevens die Verwerker in haar opdracht verwerkt beschouwd als Verwerkingsverantwoordelijke in de zin van de AVG. Verwerker is Verwerker in de zin van de AVG.

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

3. Verwerken van persoonsgegevens / Doeleinden van de verwerking

3.1 Verwerker zal de Persoonsgegevens uitsluitend verwerken op basis van de schriftelijke instructies van Verwerkingsverantwoordelijke in het kader van de uitvoering van de Overeenkomst en de te verlenen Diensten, dan wel in verband met een wettelijke verplichting. De Hoofdovereenkomst en de daarbij behorende gegevens zijn als volgt gedefinieerd:

Project Voorbeeldproject

Omschrijving verwerkingsactiviteiten:

Voorbeeld van de verwerkingsactiviteiten

Verwerkingsdoel:

Voorbeeld van het verwerkingsdoel

Subverwerkers:

De algemene subverwerkers van eyetractive zijn van toepassing. Een overzicht daarvan wordt op verzoek aangeleverd. Daarnaast zijn, specifiek voor dit project, deze aanvullende subverwerkers van toepassing:

Voorbeeld subverwerkers: x, y en z.

Verwerkingslocatie:

Online (servers binnen nederland, zie beveiligingsbeleid)

Bewaartermijn:

Standaard, zie beveiligingsbeleid

Binddatum verwerking:

01-01-2022

Einddatum verwerking:

-

Functionaris gegevensverwerking klant

Voorbeeld Klant

E-mail: voorbeeldklant@eyetractive.nl

Telefoon: 046 - 8700026

Adres: Heerstraat Centrum 131 6171 HV Stein

Verantwoordelijk binnen eyetractive:

Jan Huntjens

E-mail: jan@eyetractive.nl

Telefoon: 046 - 8700026

Verwerkte gegevens

Datasoort	Beoogd gebruik	Bron
Websitebezoek (waaronder IP-adres)	Functioneren van de website	Bezoeker van voorbeeldsysteem
Naam	Gebruikersautorisaties	Beheerder van voorbeeldsysteem
E-mailadres (of andere adres voor elektronische communicatie)	Gebruikersautorisaties	Beheerder van voorbeeldsysteem
Inloggegevens (gebruikersnaam/wachtwoord, klantnummer of ander identificatienummer)	Gebruikersautorisaties	Beheerder van voorbeeldsysteem

3.2 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. De categorieën van Betrokkenen, het soort Persoonsgegevens en de aard en het doel waarvoor de Persoonsgegevens worden verwerkt zijn hierboven opgenomen.

3.3 Verwerker zal de Persoonsgegevens niet aan een Derde verstrekken, tenzij deze uitwisseling plaatsvindt in het kader van de uitvoering van de Overeenkomst, in opdracht van of met toestemming van Verwerkingsverantwoordelijke of wanneer dit noodzakelijk is om te voldoen aan een wettelijke verplichting. In dat laatste geval zal Verwerker onmiddellijk Verwerkingsverantwoordelijke inlichten, tenzij dit is verboden.

3.4 Verwerker zal de Persoonsgegevens verwerken in landen binnen de Europese Unie. Verwerkingsverantwoordelijke geeft Verwerker daarnaast toestemming voor de verwerking van persoonsgegevens in landen buiten de Europese Unie, met inachtneming van de relevante wet- en regelgeving. Verwerker zal Verwerkingsverantwoordelijke, op diens verzoek daartoe, melden om welk land of welke landen het gaat.

3.5 Indien Verwerkingsverantwoordelijke een beoordeling wenst uit te voeren van een beoogde verwerkingsactiviteit in het kader van de uitvoering van de Overeenkomst zal Verwerker alle redelijke medewerking verlenen om deze beoordeling in overeenstemming met de geldende wet- en regelgeving uit te kunnen voeren. Tevens zal Verwerker alle redelijke medewerking verlenen indien een voorafgaande raadpleging van de AP nodig is op grond van de geldende privacywetgeving.

4. Totstandkoming, duur en beëindiging

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

4.2 Verwerker zal bij beëindiging van de Overeenkomst op verzoek van Verwerkingsverantwoordelijke de Persoonsgegevens in een gangbaar formaat ter beschikking stellen aan Verwerkingsverantwoordelijke of aan een

door Verwerkingsverantwoordelijke aangewezen Derde.

4.3 Verwerker zal na overdracht van de Persoonsgegevens aan Verwerkingsverantwoordelijke de nog aanwezige Persoonsgegevens vernietigen, tenzij een langere opslag wettelijk verplicht is. Verwerker zal tevens zorgdragen voor vernietiging van de Persoonsgegevens bij de Sub-Verwerkers.

4.4 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 en de beveiligingsmaatregelen.

5. Geheimhouding

5.1 Op alle persoonsgegevens die Verwerker van Verwerkingsverantwoordelijke ontvangt en/of zelf verzamelt in het kader van deze Verwerkersovereenkomst (zie artikel 3), rust een geheimhoudingsplicht jegens derden.

Verwerker zal deze informatie niet voor een ander doel gebruiken dan waarvoor hij deze heeft verkregen, tenzij deze in een zodanige vorm is gebracht dat deze niet tot betrokkenen herleidbaar is.

5.2 Deze geheimhoudingsplicht is verder niet van toepassing:

1. voor zover Verwerkingsverantwoordelijke uitdrukkelijke toestemming heeft gegeven om de informatie aan derden te verschaffen; of
2. - indien het verstrekken van de informatie aan derden logischerwijs noodzakelijk is voor de uitvoering van de Hoofdovereenkomst of deze Verwerkersovereenkomst; en
3. - indien er een wettelijke verplichting bestaat om de informatie aan een derde te verstrekken.

6. Beveiliging persoonsgegevens

6.1 Verwerker zal passende technische en organisatorische beveiligingsmaatregelen treffen om de Persoonsgegevens te beveiligen tegen verlies en tegen onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging daarvan, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens meebrengen. De maatregelen getroffen door Verwerker zijn opgenomen in het beveiligingsbeleid (bijlage 1).

6.2 Verwerkingsverantwoordelijke stelt enkel persoonsgegevens ter verwerking aan Verwerker ter beschikking, indien Verwerkingsverantwoordelijke kennis heeft genomen van de beveiligingsmaatregelen die getroffen zijn en daarmee instemt. Verwerkingsverantwoordelijke en Verwerker zijn mede verantwoordelijk voor de naleving van de door Partijen afgesproken maatregelen.

6.3 In bijlage 1 zijn de afspraken tussen Partijen vastgelegd over de concrete technische en organisatorische beveiligingsmaatregelen die Verwerker treft. Deze maatregelen worden periodiek geëvalueerd en indien nodig aangepast.

7. Controle/audit

7.1 Verwerker verstrekt Verwerkingsverantwoordelijke op aanvraag een rapport of een verklaring van de staat van de technische en organisatorische maatregelen die Verwerker heeft getroffen ten aanzien van de beveiliging van de Persoonsgegevens. Bij het aangaan van de Verwerkersovereenkomst zal verwerker een kopie verstrekken van het meest recente rapport of verklaring (bijlage 1).

7.2 Verwerkingsverantwoordelijke heeft het recht om op eigen kosten audits uit te laten voeren door een onafhankelijke ICT-deskundige die aan geheimhouding is gebonden ter controle van naleving van alle punten uit deze Verwerkersovereenkomst. De door Eyetractive gemaakte kosten, waaronder werkuren, zijn voor rekening van Verwerkingsverantwoordelijke.

7.3 Deze audit vindt uitsluitend plaats nadat Verwerkingsverantwoordelijke de bij Verwerker aanwezige rapportages heeft opgevraagd, beoordeeld en redelijke argumenten aanbrengt die een door Verwerkingsverantwoordelijke geïnitieerde audit alsnog rechtvaardigen. Een dergelijke audit wordt gerechtvaardigd wanneer de bij Verwerker aanwezige soortgelijke rapportages geen of onvoldoende uitsluitsel geven over het naleven van deze Verwerkersovereenkomst door Verwerker. De door Verwerkingsverantwoordelijke geïnitieerde audit vindt niet vaker dan één keer per jaar plaats.

7.4 Verwerker zal aan de audit meewerken en alle voor de audit redelijkerwijs relevante informatie, inclusief ondersteunende gegevens zoals systeemlogs, en medewerkers zo tijdig mogelijk en binnen een redelijke termijn, tenzij een spoedeisend belang zich hiertegen verzet, ter beschikking stellen.

7.5 De bevindingen naar aanleiding van de uitgevoerde audit zullen door Partijen in onderling overleg worden beoordeeld en, naar aanleiding daarvan, al dan niet worden doorgevoerd door één van de Partijen of door beide Partijen gezamenlijk.

8. Beveiligingsincidenten/meldplicht

8.1 Verwerker informeert Verwerkingsverantwoordelijke zo spoedig mogelijk en in ieder geval binnen 36 uur nadat Verwerker kennis heeft genomen van een Beveiligingsincident met betrekking tot de verwerking van de Persoonsgegevens.

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

8.3 Partijen leggen hun afspraken over de informatie-uitwisseling in verband met incidenten vast in een "Procedure Meldplicht Datalekken" in bijlage 2. Deze bijlage kan te allen tijde in overleg door Partijen worden gewijzigd. De bijlage zal in ieder geval worden aangepast indien de regelgeving omtrent de Meldplicht Datalekken of de uitleg daarvan wijzigt.

9. Verzoeken van Betrokkenen

9.1 Indien Verwerker een verzoek of bezwaar van een Betrokkene ontvangt, zoals een verzoek om informatie,

inzage, rectificatie, gegevenswissing, verwerkingsbeperking of overdracht van de Persoons-gegevens, stuurt Verwerker dat verzoek onmiddellijk door naar Verwerkingsverantwoordelijke.

9.2 Verwerker verleent Verwerkingsverantwoordelijke alle redelijke medewerking om ervoor te zorgen dat Verwerkingsverantwoordelijke binnen de wettelijke termijnen kan voldoen aan de verplichtingen op grond van de geldende wet- en regelgeving. Partijen zullen in gezamenlijk overleg afspraken maken over de redelijke verdeling van de kosten die hiermee gemoeid zijn.

10. Sub-Verwerkers

10.1 Verwerker heeft bij de verwerking van de Persoonsgegevens de mogelijkheid om Sub-Verwerkers in te schakelen.

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. Verwerker zal in ieder geval iedere Sub-Verwerker contractueel de geheimhoudingsverplichtingen, meldingsverplichtingen en beveiligingsmaatregelen na laten leven met betrekking tot de verwerking van de Persoonsgegevens.

11. Toegang tot de Persoonsgegevens

11.1 De zeggenschap over de Persoonsgegevens blijft volledig berusten bij Verwerkingsverantwoordelijke. Op verzoek van Verwerkingsverantwoordelijke zal Verwerker (een deel van) de Persoonsgegevens in gangbaar formaat ter beschikking stellen aan Verwerkingsverantwoordelijke.

11.2 Verwerker zal ervoor zorgdragen dat Verwerkingsverantwoordelijke te allen tijde toegang behoudt tot de Persoonsgegevens en zal in geval van een geschil tussen Partijen deze toegang niet blokkeren. Verwerker zal maatregelen treffen om ervoor te zorgen dat Verwerkingsverantwoordelijke ook in geval van faillissement of surséance van betaling van Verwerker toegang blijft houden tot de Persoonsgegevens.

12. Aansprakelijkheid en vrijwaring

12.1 Indien Verwerker tekortschiet in de nakoming van de Overeenkomst is Verwerker aansprakelijk voor de directe schade en kosten die Verwerkingsverantwoordelijke daardoor lijdt of heeft geleden.

12.2 Verwerker vrijwaart Verwerkingsverantwoordelijke voor boetes en/of dwangsommen van of namens de AP en/of andere bevoegde autoriteiten die aan Verwerkingsverantwoordelijke worden opgelegd en/of voor schadeclaims van Betrokkenen of Opdrachtgevers, indien deze volledig zijn toe te rekenen aan Verwerker.

13. Wijziging Verwerkersovereenkomst

13.1 In geval van wijzigingen in de Diensten, regelgeving of andere relevante omstandigheden 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.

13.2 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.

14. Toepasselijk recht

14.1 Op deze Verwerkersovereenkomst is uitsluitend Nederlands recht van toepassing.

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

bijlage 1

eyetractive.

informatie
& beveiliging

Een beveiligingsbeleid...?

Als wij werkzaamheden voor je uitvoeren, vertrouw je ons met jouw gegevens en die van je klanten. Het is onze verantwoordelijkheid om daar op een juiste manier mee om te gaan, en om je inzicht te geven in hoe we dat doen.

In dit document zetten we onze richtlijnen t.a.v. de beveiliging die we hanteren op een rijtje. Wel zo duidelijk! Mocht je nog vragen hebben naar aanleiding van dit document, neem dan zeker even contact met ons op!

Inhoudsopgave

Pagina 4

Jouw gegevens

Pagina 8

Onze werkplekken

Pagina 12

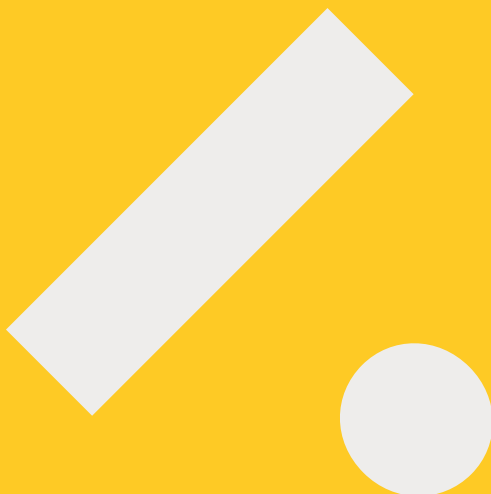
Onze servers

Pagina 16

De backups

Pagina 18

Onze medewerkers



Jouw gegevens.

In het kader van de werkzaamheden die eyetractive uitvoert voor haar klanten, worden vaak gegevens aangeleverd en verwerkt. We maken onderscheid tussen drie soorten gegevens:

1. Klantgegevens
2. (Privacy)gevoelige informatie (vertrouwelijk)
3. Overige gegevens

1. Klantgegevens

Onder klantgegevens verstaan we jouw NAW- en bedrijfsgegevens die wij opslaan t.b.v. de (administratieve) afhandeling en nazorg rondom het uitvoeren van een overeenkomst.

Bijvoorbeeld: Je (bedrijfs)naam, KuK- en BTW-nummer, factuuradres.

Verwerking

Je gegevens worden verwerkt in onze interne systemen en komen tot uiting op bijvoorbeeld offertes en facturen. Deze gegevens slaan we op voor onbepaalde termijn.

Na het beëindigen van onze samenwerking

Op verzoek verwijderen we jouw klantgegevens na het beëindigen van onze samenwerking en zodra de wettelijk verplichte bewaartermijnen verstreken zijn.

We gaan zorgvuldig met je gegevens om
en bewaren (privacy)gevoelige informatie
niet langer dan strikt noodzakelijk.

2. (Privacy)gevoelige informatie (vertrouwelijk)

Deze aanduiding geven wij en/of jij aan informatie die persoonsgegevens bevat of een sterk vertrouwelijk karakter heeft.

Bijvoorbeeld: Een lijst van e-mailadressen of een Excel bestand met financiële informatie. Of een willekeurig ander document door u aangemerkt als 'vertrouwelijk'.

Aanduiding vertrouwelijk

Wanneer je gegevens aanlevert die jij als vertrouwelijk beschouwt, dan verwachten we dat jij dat duidelijk aangeeft. Wanneer wij informatie ontvangen met persoonsgegevens (bijv: NAW-gegevens, e-mailadressen of IP adressen), dan zullen wij deze informatie aanmerken als (privacy)gevoelig.

We verwachten in beide gevallen dat de aanlevering geschiedt via de daarvoor bestemde oplossing (zie 'Aanlevering' hieronder). Wanneer je ons (privacy)gevoelige informatie stuurt via een andere weg, bijvoorbeeld een e-mail, dan zullen we de ontvangen informatie per direct verwijderen en je vragen om de informatie alsnog via onderstaande oplossing aan te leveren.

Aanlevering

Wanneer je persoonsgegevens of anderszins gevoelige informatie wil aanleveren ter verwerking, vereisen we dat deze informatie op een veilige manier aangeleverd wordt. Eyetractive biedt hiertoe een voorziening: Als klant kun je inloggen op het eyetractive klantportaal op <https://klanten.eyetractive.nl>. Daar kun je vervolgens dit soort gegevens uploaden. De aanlevering geschiedt daarmee digitaal over een beveiligde en versleutelde verbinding. Informatie over de aanlevering en verdere verwerking door ons wordt bijgehouden en inzichtelijk gemaakt voor jou.

Verwerking

Wanneer je ons gegevens hebt aangeleverd via de beveiligde online omgeving, worden ze tijdelijk bewaard op één van onze servers. Zodra wij de gegevens gaan verwerken, worden ze ingeladen op een werkplek en na verwerking

verwijderd van beide locaties. De status van verwerking en – uiteindelijk – het verwijderen van de aangeleverde gegevens, wordt bijgehouden in het eyetractive klantportaal en is daarmee voor jou inzichtelijk.

Aflevering

Indien door jou aangevraagd, kan eyetractive vertrouwelijke informatie in de vorm van exports aan je sturen. Aflevering van bestanden met vertrouwelijke informatie of persoonsgegevens zal altijd plaatsvinden via het klantportaal. Je ontvangt via e-mail een bericht dat er bestanden klaar staan. Na inloggen op het klantportaal download je de bestanden via een versleutelde en beveiligde verbinding. Bestanden die eyetractive voor je klaar zet ter aflevering, kennen een beperkte houdbaarheid: bestanden worden automatisch verwijderd 7 dagen na uploaden.

3. Overige gegevens

Alle overige gegevens die we verwerken voor je.

Bijvoorbeeld: Teksten of foto(grafisch) materiaal ter publicatie, productinformatie t.b.v. het vullen van een webshop. Of andere inhoudelijke informatie niet aangemerkt als vertrouwelijk.

Aanlevering

Voor alle overige gegevens accepteren we uitsluitend een digitale aanlevering. Voor gegevens die geen strikte geheimhouding vereisten, volstaat aanleveren via:

- een e-mail met bijlage
- een transfer via een dienst als OneDrive of WeTransfer

We accepteren geen fysieke dragers zoals USB sticks, CD/DVD's of externe harde schijven.

Na het beëindigen van onze samenwerking

Eyetractive bewaart deze gegevens zolang we samen werken. Na het beëindigen van onze samenwerking zullen je overige gegevens, na een onbepaalde termijn, verwijderd worden. Op verzoek dragen we er zorg voor dat deze gegevens binnen 14 dagen verwijderd worden.

Jouw **gegevens**: in een notendop.

We gaan zorgvuldig met je gegevens om en bewaren (privacy)gevoelige informatie niet langer dan strikt noodzakelijk.

Vertrouwelijk en/of (privacy)gevoelig

Wanneer je ons informatie aanlevert die vertrouwelijk is, gaan we er vanuit dat jij deze gegevens duidelijk aanmerkt als vertrouwelijk. Wanneer de door jou aangeleverde informatie persoonsgegevens bevat, dan beschouwen wij dit automatisch als privacy-gevoelig.

Beveiligd aanleveren

Lever vertrouwelijke of (privacy)gevoelige informatie aan via het klantportaal op <https://klanten.eyetractive.nl>.

Digitaal aanleveren

Lever ons bij voorkeur alles digitaal aan. We accepteren geen fysieke dragers zoals USB sticks, CD/DVD's of externe hdd's.



Onze werkplekken.

Fysieke werkplekken

De werkzaamheden die we voor je uitvoeren, voeren we te allen tijde uit op een daarvoor aangemerkte 'werkplek'. Dat is veelal een vaste fysieke werkplek bij ons op locatie, maar dat kan ook een plek op jouw locatie zijn, wanneer we je daar ondersteunen.

[Toegang](#)

In het geval van een vaste werkplek, bijvoorbeeld bij ons op locatie of een thuiswerkplek, dan wordt toegang tot deze werkplek verschaft op persoonsniveau. In het geval dat we je ondersteunen op locatie (en dus werken vanaf een flexibele werkplek), ben jij verantwoordelijk voor het verschaffen van fysieke toegang.

[Clean Desk Policy](#)

Op het einde van de werkdag wordt de werkplek geordend en opgeruimd achtergelaten. We zorgen ervoor dat alle gevoelige en/of vertrouwelijke informatie in hardcopy of elektronische vorm bij het verlaten van de werkplek veilig opgeborgen is en niet toegankelijk voor onbevoegden.

In het geval dat we je ondersteunen op locatie, dan verwachten we dat er een opgeruimde werkplek ter beschikking gesteld wordt, waar zich geen (privacy) gevoelige gegevens bevinden.

Door bewust om te gaan met onze werkplekken
en apparatuur houden we grip op jouw en onze informatie.

[Paperless culture](#)

We vermijden het gebruik van papier en hardcopy gegevens; we werken zo veel als mogelijk digitaal.

[Printergebruik](#)

Afdrukken met (privacy)gevoelige informatie worden niet onbeheerd in een printer achtergelaten. We vermijden het gebruik van papier en hard-copy gegevens en we werken zo veel als mogelijk digitaal.

[Netwerk](#)

Toegang tot het draadloos of bekabelde netwerk op een eyetractive locatie wordt beperkt tot de medewerkers van eyetractive. Aan derden wordt uitsluitend toegang tot internet verschaft via het gastnetwerk.

[Afvoeren van \(privacy\)gevoelige gegevens](#)

Bij het afvoeren van hardcopy (privacy)gevoelige gegevens wordt gebruik gemaakt van een papiershredder indien aanwezig. Op onze vaste werkplekken is deze voorziening aanwezig. In het geval dat we je ondersteunen op locatie, ben jij verantwoordelijk voor het veilig afvoeren van deze gegevens.

Computergebruik

Onze werkzaamheden voeren we uitsluitend uit op computers aangemerkt als onze bedrijfsapparatuur. In het geval van onze fysieke werkplekken, zijn dan onze workstations. In het geval van ondersteuning op locatie, is dat veelal één van onze bedrijfslaptops. We hanteren de volgende regels omtrent het gebruik van deze apparatuur.

[Clear Screen Policy](#)

Bij afwezigheid worden computerwerkplekken vergrendeld. Op het einde van de werkdag worden computerwerkplekken afgesloten indien mogelijk.

[Full-disk encryptie](#)

We verwerken en bewaren jouw gegevens alleen op schijven die versleuteld zijn d.m.v. full-disk encryptie technologieën zoals Bitlocker.

Geen (onbeveiligde) externe dragers

We vermijden het gebruik van externe dragers zoals USB sticks, optische media, of externe harde schijven. We maken in het geheel geen gebruik van onbeveiligde dragers voor (privacy)gevoelige of vertrouwelijke informatie.

Updates en antivirus

Onze computers worden voorzien van een operating system (OS) dat officiële ondersteuning geniet. Dit OS wordt up-to-date gehouden en voorzien van een up-to-date antivirus oplossing.

(Privacy)gevoelige of vertrouwelijke informatie op mobiele apparaten

Er wordt in de regel geen (privacy)gevoelige of vertrouwelijke informatie verwerkt op onze laptops. Indien dit wel het geval is, dan wordt de apparatuur niet onbemand achter gelaten totdat de informatie in kwestie vernietigd is.

Openbare netwerken

Er wordt in de regel geen gebruik gemaakt van onbeveiligde netwerken. Wanneer dat wel het geval is, werken we uitsluitend via beveiligde verbindingen.

Overige apparatuur

Er zijn mogelijk andere apparaten die gebruikt worden door eyetractive medewerkers voor taken als het uitlezen van e-mail (bijvoorbeeld: smartphones of tablets). Indien een eyetractive account ingeladen wordt op een dergelijk apparaat, is het een vereiste dat de toegang tot het apparaat of het account afgeschermd wordt met een wachtwoord, pincode of biometrische identificatie.

Privacy(gevoelige) of vertrouwelijke informatie wordt niet verwerkt op deze apparaten (uitsluitend op bedrijfsapparatuur).

Onze **werkplekken**: in een notendop.

We verwerken (privacy)gevoelige informatie uitsluitend op aangewezen werkplekken en aangewezen bedrijfsapparatuur.

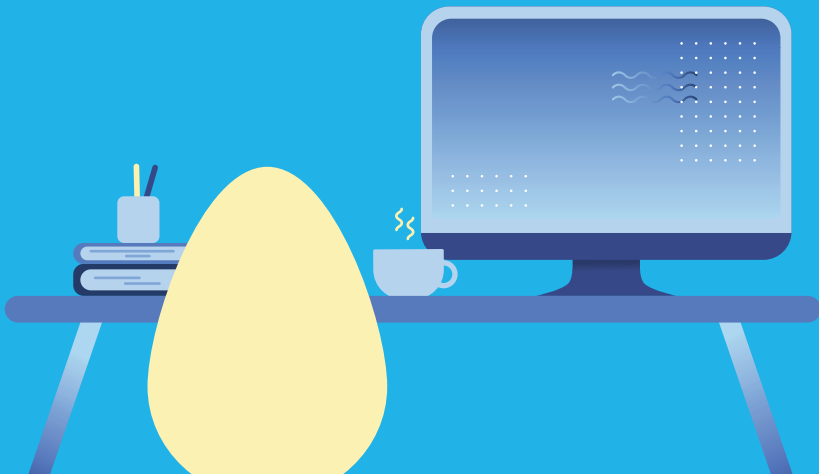
Fysieke werkplekken

We werken veelal vanuit onze vaste werkplekken bij ons op locatie, maar we kunnen je ook ondersteunen op jouw locatie.

In beide gevallen werken we in een opgeruimde en geordende omgeving en vermijden we het werken met hard-copy gegevens.

Beveiligde apparatuur

Onze apparatuur is te allen tijde beveiligd en wordt niet onvergrendeld verlaten. We zijn selectief in het verlenen van toegang.



Onze servers.

Wij maken gebruik van servers voor diverse doeleinden, bijvoorbeeld voor het hosten van websites en webapplicaties, het afhandelen van e-mailverkeer en het uitvoeren van geautomatiseerde back-up taken.

Toegang - beheer

Wanneer er beheer-taken uitgevoerd worden op onze servers, gebeurt dit uitsluitend via een beveiligde en versleutelde verbinding vanaf onze werkplekken. De accounts waarmee we werken zijn te allen tijde beveiligd met sterke en unieke wachtwoorden.

Fysiek beheer

Voor het fysieke beheer van onze servers werken we samen met vertrouwde leveranciers en datacentra binnen Nederland. De datacentra waarin de servers geplaatst zijn, gaan zorgvuldig om met hun beveiliging. De datacentra bezitten de volgende certificeringen:

ISO 9001

ISO 27001

ISO 14001

NEN 7510

PCI DSS

Toegang voor derden

Er wordt in de regel geen toegang verschaft aan derden in het kader van beheertaken. Wanneer dit wel noodzakelijk is, zal er toegang verschaft worden op persoonsniveau en wordt de toegang beperkt tot hetgeen nodig is voor het uitvoeren van de werkzaamheden.

Onze web-, mail- en back-up servers zijn geplaatst in een beveiligde omgeving, zowel digitaal als fysiek.

Toegang - Operationeel

Er kan toegang verschaft worden aan derden tot bepaalde onderdelen en protocollen op onze servers in een operationeel kader. Toegang wordt in dat geval verschaft op persoonsniveau en voor beperkte onderdelen.

Toegang tot een klantomgeving

Wanneer er toegang verschaft wordt tot een omgeving met gegevens van een specifieke klant, wordt die toegang uitsluitend verstrekt aan de klant, via een beveiligd protocol en sterke, unieke, wachtwoorden. Indien de klant zelf de mogelijkheid heeft om het wachtwoord te wijzigen, dan raden we aan z.s.m. een eigen wachtwoord te kiezen. De klant is in dit geval verantwoordelijk voor het hanteren van een sterk wachtwoord.

Als richtlijn voor een sterk wachtwoord kan het volgende aangehouden worden:

- minimaal 8 tekens lang
- een mix van hoofdletters, kleine letters, cijfers en leestekens
- bevat geen voor de hand liggende informatie als geboortedata of adressen
- een uniek wachtwoord dat op geen enkele andere plek gebruikt wordt

Update-beleid

Onze servers zijn voorzien van een operating system (OS) dat officiële ondersteuning geniet. Reguliere updates worden periodiek doorgevoerd.

Wanneer kritieke beveiligingslekken ontdekt worden in de gebruikte software, worden de patches daarvoor na uitgifte z.s.m. aangebracht.

Onze **servers**: in een notendop.

Onze web-, mail- en back-up servers zijn geplaatst in een beveiligde omgeving, zowel digitaal als fysiek.

Fysieke locatie

We werken samen met vertrouwde leveranciers en gecertificeerde datacentra binnen Nederland voor het fysieke beheer van onze servers.

Toegang

We verlenen in de regel geen toegang aan derden en werken uitsluitend via beveiligde verbindingen en accounts met unieke, sterke wachtwoorden.

Updates

Servers worden bijgewerkt via een update-beleid om optimale performance en beveiliging te kunnen garanderen.



De backups.

We maken geautomatiseerd back-ups van jouw en onze gegevens on-site en naar diverse off-site locaties. De inhoud van onze werkplekken en servers wordt op die manier veilig gesteld. Off-site back-ups zijn te allen tijde aanwezig op minimaal 3 fysieke locaties. Deze back-up doelen zijn, net als onze werkplekken, voorzien van full-disk encryptie. Toegang tot deze servers wordt beperkt tot onze medewerkers.

Historie

Geautomatiseerde back-up taken zorgen ervoor dat gegevens op een regelmatig interval bewaard worden. Van sommige gegevens bewaren we tevens de historie. In dat geval bewaren we de gegevens en veranderingen daarvan over een periode van 30 dagen.

(Privacy)gevoelige informatie

Wanneer (privacy)gevoelige gegevens verwijderd worden, zullen ze kort daarna automatisch verwijderd worden op de reguliere back-up doelen. Wanneer deze gegevens onderdeel uitmaken van een back-up taak met behoud van historie, worden ze voor een periode van 30 dagen bewaard na het lokaal verwijderen.

Zorgvuldig omgaan met gegevens beperkt zich niet alleen tot de beveiliging daarvan. Ook het veilig bewaren is van belang.

De **backups**: in een notendop.

Onze web-, mail- en back-up servers zijn geplaatst in een beveiligde omgeving, zowel digitaal als fysiek.

Off-site back-ups

Onze back-ups zijn te allen tijde beschikbaar op minimaal 3 fysieke locaties.

Historie

Sommige back-up taken worden uitgevoerd met behoud van historie.
In dat geval worden gegevens voor 30 dagen bewaard.



Onze medewerkers.

Bij in dienst treden

[Verklaring omtrent gedrag](#)

Wij verlangen van medewerkers dat zij een verklaring omtrent gedrag aanleveren bij het in dienst treden.

[Instructie en geheimhouding](#)

Onze medewerkers worden op de hoogte gebracht van het geldende beveiligingsbeleid en bijbehorende procedures. Verder worden medewerkers gehouden aan een geheimhoudingsplicht m.b.t. (privacy-)gevoelige informatie.

[Verschaffen van toegang](#)

Aan medewerkers wordt toegang verschaft tot een werkplek en tot diverse informatiesystemen. Deze toegang wordt via een password manager verleend en beperkt tot hetgeen nodig is voor het uitvoeren van de werkzaamheden.

Bij uit dienst treden

[Ontnemen van toegang](#)

Bij de beëindiging van een dienstverband zal toegang tot de werkplek en informatiesystemen ontnomen worden. Alle bedrijfsapparatuur wordt verzameld op locatie en terug in beheer genomen door eyetractive.

We nemen samen een actieve houding in in het waarborgen van een goede informatiebeveiliging.



Meer weten?

Heb je verder nog vragen over dit beleid of de manier waarop we jouw gegevens verwerken? Neem dan contact op met ons:

✉ info@eyetractive.nl

📞 046 - 870 00 26

📄 Heerstraat Centrum 131
6171 HV Stein



Bijlage 2 – Procedure meldplicht datalekken

Tussen partijen zijn met betrekking tot de meldplicht datalekken de volgende afspraken gemaakt:

1. Verwerker registreert alle Beveiligingsincidenten.
2. In geval van een Beveiligingsincident informeert Verwerker Verwerkingsverantwoordelijke zo spoedig mogelijk, in ieder geval binnen 36 uur nadat Verwerker kennis heeft genomen van het Beveiligingsincident.
3. Verwerker zal alle relevante informatie over het incident melden aan de hand van de hieronder opgenomen vragenlijst.
4. Verwerkingsverantwoordelijke zal beoordelen of een melding verricht dient te worden bij de AP en of Betrokkenen geïnformeerd dienen te worden.

Vragenlijst Beveiligingsincident – bij de Procedure Meldplicht Datalekken

De contactpersoon bij Verwerkingsverantwoordelijke voor de meldplicht datalekken zijn vermeld in de verwerkersovereenkomst onder artikel 3.1.

Verwerker zal bij een Beveiligingsincident de volgende vragen beantwoorden:

1. Geef een omschrijving van het Beveiligingsincident:

(bijvoorbeeld “gestolen laptop met klantgegevens” of “een hack op systeem [X]” of “inloggegevens verstuurd naar ontvanger Y ipv X”)

De persoonsgegevens van hoeveel personen zijn getroffen door het Beveiligingsincident?

(geef een minimum en maximum aantal aan)

2. Omschrijf de groep personen waarop de Persoonsgegevens betrekking hebben.

(bijvoorbeeld sollicitanten of cliënten van Verwerkingsverantwoordelijke)

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

3. Datum en tijdstip van het incident:

(kan een vast tijdstip zijn of een periode, als dit niet bekend is "onbekend" invullen)

4. Wanneer is het beveiligingsincident ontdekt?

5. Wat is de aard van de inbreuk? Omcirkel de antwoorden en vul in waar nodig

Kan een onbevoegde de gegevens lezen: JA / NEE

Kunnen/zijn de gegevens (worden) gekopieerd door een onbevoegde: JA / NEE

Kunnen/zijn de (bron)gegevens (worden) gewijzigd (bijv. hack in het systeem): JA / NEE

Kunnen/zijn de (bron)gegevens (worden) verwijderd of vernietigd (bijv. ransom ware of brand datacenter): JA / NEE

Zijn de gegevens gestolen: JA / NEE

Overig:

(invullen, of als de aard niet bekend is: "onbekend" invullen)

6. Om welk type gegevens gaat het? Omcirkel de antwoorden en vul in waar nodig:

Naam-, adres- en woonplaatsgegevens: JA / NEE

Telefoonnummer: JA / NEE

E-mailadres of andere adres voor elektronische communicatie: JA / NEE

Inloggegevens (gebruikersnaam/wachtwoord, klantnummer of ander identificatienummer): JA / NEE, zo ja; welke gegevens zijn het:

(invullen)

Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer): JA / NEE

Burgerservicenummer (BSN) of sofinummer: 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, zo ja; welke gegevens zijn het:

(invullen)

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

Overige gegevens:

(invullen)

7. Welke gevolgen kan de inbreuk hebben voor de getroffen personen? Omcirkel de antwoorden en vul in waar nodig:

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:

(invullen)

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

9. Zijn de gelekte persoonsgegevens beveiligd? Omcirkel de antwoorden en vul in waar nodig:

Zijn de gegevens versleuteld: JA / NEE, zo ja; welke versleuteling:

(invullen)

geldt deze versleuteling voor alle persoonsgegevens of voor een deel: JA / NEE, zo ja; voor welk deel:

(invullen)

Zijn de gegevens gehasht: JA /NEE, zo ja; op welke wijze:

(invullen)

Kunnen de gegevens vanaf afstand worden gewist: JA /NEE, zo ja; is dat gebeurd en wanneer is dat gebeurd:

(invullen)

Zijn de gegevens op een andere manier onbegrijpelijk of ontoegankelijk gemaakt: JA /NEE, zo ja; op welke manier:

(invullen)

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