

# Verwerkersvoorwaarden Tribe CRM van Efficacy Nederland B.V.

## Inhoudsopgave

Verwerkersvoorwaarden voor Applicatie Programmatuur Tribe CRM van Efficacy Nederland B.V. ....	2
1. Definities.....	3
2. Ingangsdatum en duur .....	3
3. Onderwerp van deze Verwerkersvoorwaarden .....	3
4. Verplichtingen Verwerker en Verantwoordelijke .....	4
5. Geheimhoudingsplicht.....	4
6. Meldplicht datalekken en beveiligingsincidenten.....	5
7. Beveiligingsmaatregelen en controle .....	5
8. Inschakeling derden.....	6
9. Wijziging en beëindigen Verwerkersvoorwaarden .....	7
10. Aansprakelijkheid.....	8
11. Toepasselijk recht .....	10
Bijlagen.....	11

# Verwerkersvoorwaarden voor Applicatie Programmatuur Tribe CRM van Efficy Nederland B.V.

1. De besloten vennootschap met beperkte aansprakelijkheid Efficy Nederland B.V. statutair gevestigd te 's-Hertogenbosch en kantoorhoudende te (5215MX) 's-Hertogenbosch aan De Waterman 2, ingeschreven in het handelsregister onder nummer: 27247845, handelend onder de naam Tribe CRM, te dezen rechtsgeldig vertegenwoordigd door mevrouw K.I. Alleijn in de functie van operationeel directeur, hierna te noemen "Verwerker";

en

2. De klant (zoals gedefinieerd in de algemene voorwaarden en zoals omschreven in de (Partner)aanmelding, aanmelding, offerte, opdrachtbevestiging of vergelijkbare overeenkomst) zijnde de (rechts)persoon of organisatie die digitaal dan wel schriftelijk opdracht heeft verstrekt aan Verwerker voor het leveren van Programmatuur, diensten of overige zaken, hierna te noemen "Verantwoordelijke";

Gezamenlijk aan te duiden als "Partij(en)";

## Overwegende dat:

- Verantwoordelijke bepaalde vormen van verwerkingen wil laten verrichten door Verwerker, waarbij Verantwoordelijke het doel en de middelen aanwijst;
- Verwerker hiertoe bereid is en tevens bereid is verplichtingen omtrent beveiliging en andere aspecten van de Algemene Verordening Gegevensbescherming en aanverwante regelgeving en gedragscodes na te komen;
- Partijen een of meerdere overeenkomsten ("Overeenkomst(en)") hebben gesloten waarin het verwerken van persoonsgegevens onderdeel uitmaakt van de dienstverlening;
- Partijen mede gelet op het vereisten uit artikel 28 derde lid van de AVG hun rechten en plichten wensen vast te leggen in deze Verwerkersvoorwaarden;
- Waar in deze Verwerkersvoorwaarden termen worden gebruikt die overeenstemmen met definities uit artikel 4 AVG, wordt aan deze termen de betekenis van de definities uit de AVG toegekend.

## Verantwoordelijke en Verwerker komen samen overeen:

## 1. Definities

**Bijlagen:** aanhangsels bij deze Verwerkersvoorwaarden die deel uitmaken van deze Verwerkersvoorwaarden.

**Toezichthouder:** de Autoriteit Persoonsgegevens (AP) is het zelfstandig bestuursorgaan dat in Nederland bij wet als toezichthouder is aangesteld voor het toezicht op het verwerken van persoonsgegevens.

**Verantwoordelijke:** 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.

**Verwerker:** een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van Verantwoordelijke persoonsgegevens verwerkt. Degene die ten behoeve van Verantwoordelijke persoonsgegevens verwerkt, in opdracht van Verwerker, is een sub-Verwerker.

## 2. Ingangsdatum en duur

2.1. Deze Verwerkersvoorwaarden gaan in op het moment van het aangaan van de Overeenkomst en duren voort zolang Verwerker als Verwerker van persoonsgegevens optreedt in het kader van de door Verantwoordelijke ter beschikking gestelde persoonsgegevens voor verwerking op het platform van Verwerker.

## 3. Onderwerp van deze Verwerkersvoorwaarden

3.1. Verwerker verwerkt de door of via Verantwoordelijke ter beschikking gestelde persoonsgegevens uitsluitend in opdracht van Verantwoordelijke in het kader van de uitvoering van de hoofdovereenkomst. De door Verwerker uit te voeren werkzaamheden waar deze Verwerkersvoorwaarden betrekking op hebben, worden nader omschreven in bijlage 2. Verwerker zal de persoonsgegevens niet voor enig ander doel verwerken, behoudens afwijkende wettelijke verplichtingen.

3.2. Verwerker verbindt zich om in het kader van die werkzaamheden de door of via Verantwoordelijke ter beschikking gestelde persoonsgegevens zorgvuldig te verwerken.

## 4. Verplichtingen Verwerker en Verantwoordelijke

- 4.1. Verwerker verwerkt gegevens ten behoeve van Verantwoordelijke, in overeenstemming met diens (schriftelijke) instructies.
- 4.2. Verantwoordelijke garandeert Verwerker dat de verwerking van persoonsgegevens rechtmatig geschiedt. Indien Verwerker van mening is dat Verantwoordelijke in strijd handelt met de AVG, stelt Verwerker Verantwoordelijke daarvan op de hoogte.
- 4.3. Verwerker heeft geen zeggenschap over de ter beschikking gestelde persoonsgegevens. Zo neemt hij geen beslissingen over ontvangst en gebruik van de gegevens, de verstrekking aan derden en de duur van de opslag van gegevens. De zeggenschap over de persoonsgegevens verstrekt onder deze Verwerkersvoorwaarden komt nimmer bij Verwerker te berusten.
- 4.4. Verwerker zal bij de verwerking van persoonsgegevens in het kader van de in artikel 3 genoemde werkzaamheden, handelen in overeenstemming met de toepasselijke wet- en regelgeving betreffende de verwerking van persoonsgegevens. Verwerker zal alle redelijke instructies van (de contactpersoon van) Verantwoordelijke opvolgen, behoudens afwijkende wettelijke verplichtingen. Indien deze afwijkende wettelijke verplichtingen er zijn wordt Verantwoordelijke hiervan, voorafgaand aan de verwerking, schriftelijk op de hoogte gebracht door Verwerker.
- 4.5. Verwerker stelt Verantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG, meer in het bijzonder de rechten van betrokkenen, zoals, maar niet beperkt tot een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet. De redelijkerwijs daarmee gepaard gaande kosten komen voor rekening van Verantwoordelijke.
- 4.6. Verwerker werkt op verzoek van Verantwoordelijke te allen tijde mee aan een gegevensbeschermings-effectbeoordeling ((D)PIA). De redelijkerwijs daarmee gepaard gaande kosten komen voor rekening van Verantwoordelijke.

## 5. Geheimhoudingsplicht

- 5.1. Personen in dienst van, dan wel werkzaam ten behoeve van Verwerker, evenals Verwerker zelf, zijn verplicht tot geheimhouding met betrekking tot de

persoonsgegevens waarvan zij kennis kunnen nemen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht. De medewerkers van Verwerker is hiertoe geheimhouding opgelegd.

- 5.2. Indien Verwerker op grond van een wettelijke verplichting gegevens aan een derde dient te verstrekken, zal Verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal Verwerker Verantwoordelijke onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren, tenzij wettelijke bepalingen dit verbieden.

## 6. Meldplicht datalekken en beveiligingsincidenten

- 6.1. Verwerker zal Verantwoordelijke zo spoedig mogelijk -afgezet tegen de termijn die geldt voor een eventuele meldingsplicht van Verantwoordelijke- informeren over alle relevante inbreuken op de beveiliging, onverminderd de verplichting de gevolgen van dergelijke inbreuken en incidenten zo snel mogelijk ongedaan te maken dan wel te beperken. Daarbij verschaft Verwerker, zo mogelijk, de informatie aan Verantwoordelijke zoals omschreven in bijlage 3.
- 6.2. Verwerker beschikt over een gedegen plan van aanpak betreffende de omgang met en afhandeling van inbreuken en zal Verantwoordelijke, op diens verzoek, inzage verschaffen in het plan.
- 6.3. Verwerker is niet verplicht tot het doen van een melding aan de Toezichthouder. Deze verantwoordelijkheid berust bij Verantwoordelijke.
- 6.4. Verwerker zal alle noodzakelijke medewerking verlenen aan het zo nodig, op de kortst mogelijke termijn, verschaffen van aanvullende informatie aan de Toezichthouder en/of betrokkene(n). Daarbij verschaft Verwerker in ieder geval de informatie, zoals beschreven in bijlage 3, aan Verantwoordelijke.
- 6.5. Verwerker houdt een overzicht bij van alle (vermoedens van) inbreuken op de beveiliging, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen.

## 7. Beveiligingsmaatregelen en controle

- 7.1. Verwerker neemt alle passende technische en organisatorische maatregelen om de persoonsgegevens welke worden verwerkt ten dienste van Verantwoordelijke te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van

onrechtmatige verwerking. De wijze van beveiliging wordt nader omschreven in bijlage 1.

- 7.2. Verantwoordelijke is gerechtigd de verwerking van persoonsgegevens door onafhankelijke en onder geheimhouding werkende deskundigen te (doen) controleren, doch maximaal één maal per jaar.
- 7.3. Verantwoordelijke zal de controle slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan Verwerker en nadat bestaande rapporten van Verwerker als onvoldoende zijn beoordeeld.
- 7.4. Verwerker zal binnen een redelijke termijn, van minimaal twee weken, Verantwoordelijke, of de door Verantwoordelijke ingeschakelde derde, te voorzien van de verlangde informatie. Hierdoor kan Verantwoordelijke, of de door Verantwoordelijke ingeschakelde derde, zich een oordeel vormen over de naleving door Verwerker van deze Verwerkersvoorwaarden. Verantwoordelijke, of de door Verantwoordelijke ingeschakelde derde, is gehouden alle informatie betreffende deze controles vertrouwelijk te behandelen.
- 7.5. Verwerker staat ervoor in, de door Verantwoordelijke of ingeschakelde derde, aangegeven passende maatregelen ter verbetering binnen de daartoe door Verantwoordelijke te bepalen redelijke termijn uit te voeren.
- 7.6. Naast rapportages van Verwerker en controles door Verantwoordelijke of controlerende instantie in opdracht van Verantwoordelijke, kunnen beide partijen ook overeenkomen gebruik te maken van een ISO 27001 certificering opgesteld door een onafhankelijke externe deskundige.
- 7.7. De kosten van de controle worden gedragen door de partij die de kosten maakt.

## 8. Inschakeling derden

- 8.1. Verwerker vermeldt de, ten tijde van het sluiten van de Overeenkomst, reeds bekende derden, die persoonsgegevens voor Verwerker verwerken, in bijlage 4. Verantwoordelijk geeft hierbij algemene toestemming voor de inschakeling van derden. Verwerker houdt na de start van de werkzaamheden Verantwoordelijke op de hoogte van de inschakeling van nieuwe derden.
- 8.2. Verwerker garandeert dat deze derden schriftelijk voldoende plichten op zich nemen als tussen Verantwoordelijke en Verwerker is overeengekomen en zal

Verantwoordelijke, op diens verzoek, inzage verschaffen in de overeenkomsten met deze derden waarin deze plichten zijn opgenomen.

- 8.3. Verwerker mag de persoonsgegevens uitsluitend verwerken binnen de Europese Economische Ruimte (EER). Doorgifte naar andere landen buiten de EER is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van Verantwoordelijke en met inachtneming van de toepasselijke wet- en regelgeving.
- 8.4. Verwerker houdt een actueel register bij van de door hem ingeschakelde derden en onderaannemers waarin de identiteit, vestigingsplaats en een beschrijving van de werkzaamheden van de derden of onderaannemers zijn opgenomen, alsmede eventuele door Verantwoordelijke gestelde aanvullende voorwaarden. Dit register zal als bijlage 4 aan deze Verwerkersvoorwaarden worden toegevoegd en zal door Verwerker actueel worden gehouden.

## 9. Wijziging en beëindigen Verwerkersvoorwaarden

- 9.1. Verwerker is gerechtigd wijzigingen in Verwerkersvoorwaarden door te voeren. Verantwoordelijke heeft daarna dertig dagen de tijd om aan te geven dat hij niet akkoord is. Zonder tegenbericht van Verantwoordelijke zijn de wijzigingen door Verantwoordelijke geaccepteerd.
- 9.2. Na beëindiging van de overeenkomst zoals omschreven in de voorwaarden Tribe CRM zal (i) Verwerker alle in het kader van deze Verwerkersvoorwaarden ter beschikking gestelde persoonsgegevens aan Verantwoordelijke ter beschikking stellen, overeenkomstig het daartoe in de voorwaarden Tribe CRM bepaalde inzake het extraheren van persoonsgegevens (ii) de persoonsgegevens die hij van Verantwoordelijke heeft ontvangen op alle locaties vernietigen, in welke vorm dan ook, tenzij dwingendrechtelijke bepalingen vereisen dat bepaalde gegevens bewaard moeten blijven. De daarmee gepaard gaande redelijke kosten komen voor rekening van Verwerker.
- 9.3. Verwerker zal te allen tijde de in het vorig lid beschreven recht op overdraagbaarheid van gegevens conform artikel 20 AVG waarborgen, zodanig dat er geen sprake is van verlies van (delen van) de gegevens.
- 9.4. Verwerker zal Verantwoordelijke tijdig informeren over wijzigingen in deze Verwerkersvoorwaarden, als een wijziging in regelgeving of een wijziging in de uitleg van regelgeving daartoe aanleiding geeft.

9.5. Indien een Partij tekortschiet in de nakoming van een overeengekomen verplichting, kan de andere Partij haar in gebreke stellen waarbij de nalatige partij alsnog een redelijke termijn voor de nakoming wordt gegund. Blijft nakoming ook dan uit dan is de nalatige partij in verzuim. Ingebrekestelling is niet nodig wanneer voor de nakoming een fatale termijn geldt, nakoming blijvend onmogelijk is of indien uit een mededeling dan wel de houding van de andere partij moet worden afgeleid dat deze in de nakoming van haar verplichting zal tekortschieten.

9.6. Verantwoordelijke is gerechtigd, onverminderd hetgeen daartoe bepaald is in Verwerkersvoorwaarden en de daarmee samenhangende hoofdovereenkomst, en onverminderd hetgeen overigens in de wet is bepaald, de uitvoering van deze Verwerkersvoorwaarden door middel van een aangetekend schrijven op te schorten, dan wel zonder rechterlijke tussenkomst met onmiddellijke ingang geheel of gedeeltelijk te ontbinden, nadat Verantwoordelijke constateert dat:

- (a) Verwerker (voorlopige) surseance van betaling aanvraagt; of
- (b) Verwerker zijn faillissement aanvraagt of in staat van faillissement wordt verklaard; of
- (c) de onderneming van Verwerker wordt ontbonden; of
- (d) Verwerker zijn onderneming staakt; of
- (e) sprake is van een ingrijpende wijziging in de zeggenschap over de activiteiten van de onderneming van Verwerker die maakt dat het in alle redelijkheid niet van Verantwoordelijke kan worden verwacht dat zij Verwerkersvoorwaarden in stand houdt; of
- (f) op een aanmerkelijk deel van het vermogen van Verwerker beslag wordt gelegd (anders dan door verantwoordelijke); of
- (g) de Verwerker tekortschiet in de nakoming van de verplichtingen die voortvloeien uit deze Verwerkersvoorwaarden en die toerekenbare tekortkoming niet binnen 30 dagen is hersteld na een daartoe strekkende schriftelijke ingebrekestelling dan wel een van de overige situaties bedoeld in artikel 9.5 zich voordoet.

9.7. Indien de Overeenkomst(en) voortijdig wordt beëindigd zijn artikel 9 lid 2 en 3 van overeenkomstige toepassing.

## 10. Aansprakelijkheid

10.1. Verwerker is aansprakelijk op grond van het bepaalde in artikel 82 AVG, voor directe schade voortvloeiende uit het niet nakomen van deze Verwerkersvoorwaarden, daaronder begrepen wanneer bij de verwerking niet



wordt voldaan aan de specifiek tot Verwerker gerichte verplichtingen van de AVG, of indien buiten de rechtmatige instructies van Verantwoordelijke is gehandeld.

10.2. Verwerker is slechts aansprakelijk voor directe schade voor zover deze is ontstaan door werkzaamheid van Verwerker. De eventuele aansprakelijkheid van PerfectView is per gebeurtenis, waarbij een samenhangende reeks van gebeurtenissen als één gebeurtenis geldt, beperkt tot het bedrag dat door de bedrijfsaansprakelijkheidsverzekeraar van PerfectView wordt uitgekeerd. Keert de verzekeraar om welke reden dan ook niet uit, dan is de aansprakelijkheid van PerfectView per gebeurtenis, waarbij een samenhangende reeks van gebeurtenissen als één gebeurtenis geldt, beperkt tot het bedrag gelijk aan de prijs voor de Opdracht, welke gefactureerd is in het tijdvak van 12 maanden direct voorafgaande aan het schadeveroorzakende voorval.

10.3. Onder directe schade worden limitatief verstaan de schadeposten zoals opgenomen in de polisbladen van de bedrijfsaansprakelijkheidsverzekering van PerfectView.

10.4. Aansprakelijkheid voor bedrijfsschade, waaronder schade wegens gederfde winst of niet gerealiseerde besparingen, reputatieschade of andere indirecte of gevolgschade is uitgesloten. Eveneens is uitgesloten de aansprakelijkheid van PerfectView verband houdende met vermindering, vernietiging of verlies van gegevens of documenten, bijvoorbeeld bij een beveiligingsincident en/of datalek, of de voorkoming of beperking hiervan.

10.5. Bovenstaande beperkingen van de aansprakelijkheid vervallen in het geval van opzet of grove schuld van PerfectView en/of van haar tot de directie en/of bedrijfsleiding behorende leidinggevende ondergeschikten.

10.6. Indien Verwerker de in artikel 6 lid 1 van deze Verwerkersvoorwaarden neergelegde verplichting niet of niet-tijdig nakomt en de Toezichthouder Verantwoordelijke dientengevolge een bestuurlijke boete oplegt, is Verwerker aansprakelijk en zal Verantwoordelijke een contractuele boete ter hoogte van hetzelfde bedrag opleggen aan Verwerker. Deze boete is niet vatbaar voor verrekening en opschorting en laat de rechten van Verantwoordelijken op nakoming en schadevergoeding onverlet.

10.7. Indien Verwerker een sanctie krijgt opgelegd door de Toezichthouder of schade dient te vergoeden aan een betrokkene, ten gevolge van handelen of nalaten van Verantwoordelijke, vrijwaart Verantwoordelijke Verwerker en stelt deze op eerste

verzoek schadeloos voor deze sanctie of schade, waaronder mede begrepen de (juridische) kosten.

## 11. Toepasselijk recht

11.1. Op deze Verwerkersvoorwaarden en op alle geschillen die daaruit voortvloeien of daarmee samenhangen, is uitsluitend Nederlands recht van toepassing.

11.2. Alle geschillen die ontstaan naar aanleiding van deze Verwerkersovereenkomst worden beslecht op dezelfde wijze als opgenomen in de Overeenkomst waarvan de Voorwaarden van Tribe CRM deel uitmaken.

11.3. Naast deze Verwerkersvoorwaarden zijn de Voorwaarden Tribe CRM van toepassing. Ingeval van tegenstrijdigheden tussen de verschillende documenten is de volgorde als volgt: (1) Overeenkomst (2) Licentievoorwaarden Tribe CRM (3) Verwerkersvoorwaarden Tribe CRM (4) Algemene Voorwaarden Tribe CRM (5) Privacystatement.

## Bijlagen

### **Bijlage 1: Beschrijving beveiligingsmaatregelen**

Ter uitwerking van artikel 7 lid 1

### **Bijlage 2: Omschrijving werkzaamheden Verwerker**

Ter uitwerking van artikel 3 lid 1

### **Bijlage 3: Inlichtingen om incidenten te beoordelen**

Ter uitwerking van artikel 6 lid 1 en 5

### **Bijlage 4: Subverwerkersregister**

Ter uitwerking van artikel 8 lid 1 en 5

## Bijlage 1: Beschrijving beveiligingsmaatregelen Tribe CRM

Voor de definitie van de gebruikte termen wordt verwezen naar de Tribe CRM verwerkersvoorwaarden van Efficacy Nederland B.V..

In dit document worden de organisatorische en technische beveiligingsmaatregelen van de Applicatie Programmatuur Tribe CRM gedetailleerd verklaard. Nadruk ligt voornamelijk op de maatregelen die zijn gericht op de continuïteit, integriteit en beschikbaarheid van de Applicatie Programmatuur Tribe CRM.

Aangezien in de Tribe CRM applicatie persoonsgegevens worden verwerkt, zijn deze maatregelen van groot belang om een juiste mate van beveiliging te creëren zoals de AVG dit aan gegevensverwerkers voorschrijft (AVG Artikel 28).

### Organisatorische maatregelen

#### **Certificering ISO 27001**

Tribe CRM is ISO 27001:2013 gecertificeerd. Zeer actief wordt in de gehele organisatie gewerkt aan een optimale informatieveiligheid. Jaarlijks wordt door een onafhankelijke geaccrediteerde instantie de certificering beoordeeld. De hosting partner Google die als subverwerker dient, is o.a. ISO 27001, ISO 270017, ISO 27018 en SSAE 16/ISAE 3402 Type II gecertificeerd.

#### **EER (Europees Economische Regio)**

Zowel Tribe CRM als alle opslaglocaties die samen de Tribe CRM applicatie aanbieden bevinden zich in de EER. Voor de hosting maken we enkel gebruik van de fysieke Google locaties in de EER. (Waaronder datacenters in de Eemshaven in Nederland en in Saint-Ghislain in België) en voldoen geheel aan de EU-wetgeving voor gegevensbescherming.

#### **Rapportage**

Tribe CRM deelt via nieuwsberichten in de applicatie, en via e-mail berichten specifiek aan de veiligheidsfunctionaris, informatie aangaande de maatregelen en resultaten van audits en pentests met betrekking tot informatieveiligheid.

## Partners

Tribe CRM benut een selecte groep aan subverwerkers welke een gelijk belang aan beschikbaarheid, integriteit en vertrouwelijkheid hechten als Tribe CRM. Afspraken zijn bindend vastgelegd in verwerkersovereenkomsten en service level agreements.

## Verantwoordelijkheden

Alle medewerkers van Tribe CRM hebben een geheimhoudingsverklaring getekend t.a.v. alle informatie waarvan zij kennisnemen. Van alle medewerkers is en wordt periodiek een Verklaring Omtrent het Gedrag (VOG) opgevraagd voor de in hun functie toepasselijke rollen.

Periodiek worden alle medewerkers geïnformeerd over de verantwoordelijkheden ten aanzien van de informatieveiligheid. Medewerkers bezitten slechts de minimale toegangsrechten benodigd voor uitvoering van hun taken.

Binnen Tribe CRM zijn een Chief Information Security Officer en een Data Protection Officer aangesteld.

## Ontwikkeling

Beveiligingsaspecten (beschikbaarheid, integriteit en vertrouwelijkheid) zijn integraal onderdeel van de ontwikkeling bij o.a. design, development en tests. Wijzigingen worden gecontroleerd doorgevoerd in de verschillende omgevingen.

# Technische maatregelen

## Internetcommunicatie

De connectie tussen de Tribe CRM applicatie in het datacenter en het Internet is redundant uitgevoerd. Vanuit het datacenter zijn connecties opgezet naar meerdere internetknooppunten in Nederland.

Communicatie met onze de Tribe CRM applicatie wordt tijdens de overdracht versleuteld. Het netwerk en de infrastructuur hebben meerdere beveiligingslagen om onze klanten te beschermen tegen DoS-aanvallen (Denial of Service).

Het gebalanceerde netwerkverkeer is beperkt tot enkel de noodzakelijke diensten, poort HTTP (poort 80) en HTTPS (poort 443) voor de web services en SMTP (poort 25) voor de mail services zijn toegestaan in de firewall routes.

De routes kunnen enkel leiden naar servers welke de diensten ook daadwerkelijk aanbieden. De internettoegang tot de omgeving staat geen toegang voor technisch beheer of directe toegang tot de databasesystemen toe.

## Opslag

Tribe CRM wordt aangeboden op basis van het Google Cloud Platform. Voor de applicatie worden verschillende opslagmedia benut in de google cloud.

Onderstaande Google Clouddiensten benut voor Tribe CRM bevatten dataopslag:

- Google App Engine
- Google Compute Engine
- Google Kubernetes Engine
- Google Cloud SQL

## Locatie

Alle Google Clouddiensten die benut worden, worden aangeboden in de EER.

De volgende locaties worden benut:

- Europe-West4, Eemshaven, Nederland
- Europe-West1, St. Ghislain, België

De data benut in deze diensten wordt ook fysiek op deze locaties opgeslagen.

### *Europe-West1*

In het Belgische Google datacenters (2 nodes) wordt de Google App Engine dienst aangeboden.

### *Europe-West4*

In de Nederlandse Google datacenters (3 nodes) worden de Google Compute Engine , Google Kubernetes Engine en Google Cloud SQL diensten aangeboden.

Meer informatie zie : [Google regio's en zones](#)

### Encryptie

Voor alle opslagmedia wordt de data at rest versleuteld opgeslagen middels de door Google geboden versleutelingsmethodieken, met onderstaande kenmerken:

- Google gebruikt meerdere versleutelingslagen om 'data at rest' in Google Cloud-producten te beveiligen.
- Google Cloud versleutelt de 'data at rest' automatisch met een of meer versleutelingsmechanismen.
- Gegevens voor opslag worden in blokken opgedeeld en elk blok wordt versleuteld met een unieke sleutel voor gegevensversleuteling. Deze sleutels voor gegevensversleuteling worden samen met de gegevens opgeslagen en worden op hun beurt versleuteld ('verpakt') met sleutels voor gegevensversleuteling. Dit laatste type sleutels wordt alleen opgeslagen en gebruikt binnen de centrale service voor sleutelbeheer van Google. De service voor sleutelbeheer van Google is redundant en wereldwijd gedistribueerd.
- Alle gegevens die in Google Cloud Platform zijn opgeslagen, worden op opslagniveau versleuteld met AES256.
- Google gebruikt een gemeenschappelijke versleutelingsbibliotheek, Tink, om versleuteling consequent te implementeren in bijna alle Google Cloud-producten. Deze bibliotheek omvat onze FIPS 140-2-gevalideerde module [BoringCrypto](#). Omdat we deze gemeenschappelijke bibliotheek consistent gebruiken, hoeft slechts een klein team van versleutelingsdeskundigen deze nauwgezet beheerde en gecontroleerde code te implementeren en te onderhouden.

Meer informatie zie: [Versleuteling van 'data at rest' in Google Cloud](#)

### **Infrastructuur**

De infrastructuur in het datacenter is geheel redundant uitgevoerd. Alle connecties zowel aan de publieke (internet) zijde als aan de lokale beheerzijde zijn dubbel uitgevoerd. Ook de gekoppelde netwerkcomponenten als netwerk switches, firewalls en loadbalancers zijn redundant uitgevoerd.

Van de fysieke locatie tot de speciaal gebouwde servers, netwerkapparatuur, custom

beveiligingschips en softwarestack op laag niveau die op elke computer wordt uitgevoerd: de gehele hardware-infrastructuur wordt door Google beheerd, beveiligd, ontworpen en versterkt.

De verschillende omgevingen voor ontwikkeling, test, acceptatie en productie omgeving zijn geheel gescheiden opgezet.

### **Datacenters**

Tribe CRM benut de datacenters van Google, hierin wordt een gelaagd beveiligingsmodel gehanteerd met speciaal ontworpen elektronische toegangspassen, alarmsystemen, slagbomen, hekwerken, metaaldetectoren en biometrische systemen. De vloer van de datacenters is tegen indringers beveiligd met laserdetectie.

De datacenters worden 24 uur per dag beveiligd door binnen- en buitencamera's met een hoge resolutie die indringers kunnen detecteren en volgen. Alleen bevoegde werknemers met specifieke rollen hebben toegang tot de datacenters.

### **Updates**

De omgeving wordt periodiek voorzien van de service updates van de leveranciers. De updates voor de infrastructuur, opslagsystemen en cloudservices worden door Google uitgevoerd. De Tribe CRM applicatie systemen worden door Tribe CRM up to date gehouden. Tribe CRM benut in het DevOps teams een continuous delivery proces om haar applicatie snel en efficiënt te ontwikkelen. Hiermee kunnen aanpassingen in een kort cyclische wijze geïmplementeerd worden in het product.

### **Back-ups**

Iedere nacht wordt van alle data een back-up gemaakt. De back-ups worden op een gescheiden backup omgeving geplaatst en worden daar voor een periode van 3 maanden bewaard. De back-ups worden versleuteld opgeslagen.

De totale back-up retentie is 3 maanden. Verwijdering van (persoons-) gegevens vindt z.s.m. plaats op verzoek van verantwoordelijke maar zal pas leiden tot volledige vernietiging na afloop van de back-up cyclus.



## **Anti-virus**

Alle servers en (beheer-) werkplekken zijn voorzien van anti-virus software welke dagelijks wordt bijgewerkt.

## **E-Mail**

Alle uitgaande e-mail wordt door anti-spam/antivirus filters geleid om ongewenste berichten te voorkomen/te stoppen. Tribe CRM monitort het mail verkeer nauwgezet. Hiervoor wordt het mail platformen van Flowmailer ingezet.

## **Communicatie**

Gegevens worden uitsluitend uitgewisseld via cryptografisch beveiligde verbindingen. Alle communicatie tussen clients (gebruikers) en de servers wordt middels SSL versleuteld. Tribe CRM benut een SSL-certificaat met een SSL 2048 bits SHA 265 sleutel.

Maandelijks wordt gecontroleerd of de certificaten, chipers en keys die benut worden nog een A Grade scoren in de tests van SSL Labs.com om te beoordelen of er voldoende cryptografisch bescherming actief is.

## **Penetratietest**

Minimaal 1 keer per jaar wordt de Tribe CRM applicatie uitgebreid getest op kwetsbaarheden. Een zogenaamde black- en grey penetratietest wordt uitgevoerd door een onafhankelijke instantie op basis van de OWASP best practices. Tribe CRM kan hiervan op verzoek de coverletter overleggen van de laatste pentest.

## **Toegangsbeveiliging**

Toegang voor gebruikers is mogelijk op basis van complexe wachtwoorden. Complexiteit en wijzigingsbeleid van wachtwoorden is door de applicatiebeheerder in te stellen. We slaan wachtwoorden van gebruikers niet op. Tribe CRM gebruikt onomkeerbare encryptie, waardoor wachtwoorden meteen worden omgezet in een code (hash), die niet door derden kan worden ontcijferd.

Na 3 mislukte inlogpogingen binnen 5 minuten wordt een account geblokkeerd voor een bepaalde periode zodat niemand eindeloos lang een wachtwoord kan proberen te kraken.

Applicatie beheerders kun aanvullend in de applicatie instellingen IP-adressen opgeven, waarvandaan er ingelogd kan én mag worden.

Toegang tot de gegevens voor Tribe CRM is beperkt tot de door de klant aangewezen supportmedewerkers van Tribe CRM. Medewerkers van Tribe CRM zullen nooit per e-mail of telefoon vragen om vertrouwelijke gegevens zoals wachtwoord gegevens.

### **Monitoring**

De Tribe CRM applicatie wordt continue gemonitord om onderhoud, storingsherstel, capaciteit beheer, etc. adequaat en tijdig uit te kunnen voeren.

### **Logging**

In de Tribe CRM applicatie worden uitgebreide auditlog's aangelegd m.b.t. gegevenswijzigingen en systeemwijziging door gebruikers en beheerders. De log's kunnen niet aangepast of gemanipuleerd worden door gebruiker en/of beheerder.

## Bijlage 2: Omschrijving werkzaamheden verwerker Tribe CRM

Voor de definitie van de gebruikte termen wordt verwezen naar de Tribe CRM verwerkersvoorwaarden van Efficacy Nederland B.V..

### 1. Verwerkingen

Dit verwerkingsregister benoemt twee verwerkingen in het kader van de overeenkomst tussen verwerker en verantwoordelijke.

#### 1.1. Verwerking gebruikersgegevens

Doel	Gebruikersadministratie voor toegang tot de Applicatie Programmatuur door medewerkers van verantwoordelijke
Rechtsgrondslag	Uitvoering van de overeenkomst
Betrokkenen	Medewerkers van verantwoordelijke
Duur	Duur van de overeenkomst

De volgende Persoonsgegevens zullen in het kader van de Overeenkomst worden verwerkt:

- Naam, email, en organisatie (indirect afleidbaar).

Verwerker verwerkt op de volgende wijzen persoonsgegevens voor verantwoordelijke:

- Gebruikersgegevens worden opgeslagen ten behoeve van beheer door verantwoordelijke ten aanzien van de toegangscontrole van de Applicatie Programmatuur.
- Gebruikersgegevens worden gebruikt om verantwoordelijke en betrokkenen te informeren over wijzigingen en/of incidenten in de Applicatie Programmatuur zoals verwerker die aanbiedt.

Verantwoordelijke bepaalt welke Persoonsgegevens worden verwerkt.

## 1.2. Aanbieden Applicatie Programmatuur

Doel	Aanbieden van Applicatie Programmatuur met als doel het registreren van relatiegegevens van de verantwoordelijke. Met aanbieden van Applicatie Programmatuur worden tevens de hier onlosmakelijk aan verbonden verwerkingen als hosten, back-uppen, beheren, ondersteunen en ontwikkelen van de Applicatie Programmatuur bedoeld
Rechtsgrondslag	Uitvoering van de overeenkomst
Betrokkenen	Relaties, medewerkers van de geregistreerde relaties en medewerkers van de verantwoordelijke
Duur	Duur van de overeenkomst

De Applicatie Programmatuur biedt in het kader van de overeenkomst de mogelijkheid om persoonsgegevens te verwerken. Tribe CRM gaat uit van de volgende persoonsgegevens en heeft hier haar beveiligingsmaatregelen op afgestemd:

- Naam (roep-/voor-/achternaam en tussenvoegsels), geslacht, e-mail, website, telefoonnummers (mobiel, vast, skype en fax), adresgegevens (straat, huisnummer, postcode, plaats en land) en werkgever.

Verwerker verwerkt op de volgende wijzen persoonsgegevens voor verantwoordelijke:

- Gebruikersgegevens worden opgeslagen ten behoeve van relatiebeheer door verantwoordelijke als ondersteuning in de uitvoering van haar bedrijfsprocessen.
- Gegevens worden opgeslagen, onderhouden en geback-up't op het platform zodanig dat deze voor verantwoordelijke toegankelijk zijn, bij/na updates beschikbaar zijn en in geval van calamiteiten te herstellen zijn.
- Tribe CRM verspreidt geen enkel persoonsgegeven binnen haar platform aan derden.

Verantwoordelijke bepaalt welke persoonsgegevens worden verwerkt en/of de geboden beveiligingsmaatregelen afdoende zijn voor haar verwerkingen.

## Bijlage 3: Inlichtingen om incidenten te beoordelen Tribe CRM

Voor de definitie van de gebruikte termen wordt verwezen naar de Tribe CRM verwerkersvoorwaarden van Efficacy Nederland B.V..

### Meldplicht datalekken en beveiligingsincidenten

De verwerker zal alle inlichtingen verschaffen die de verwerkingsverantwoordelijke noodzakelijk acht om het incident te kunnen beoordelen. Daarbij verschaft verwerker in ieder geval de volgende informatie aan de verwerkingsverantwoordelijke:

- wat de (vermeende) oorzaak is van de inbreuk;
- wat het (vooralsnog bekende en/of te verwachten) gevolg is;
- wat de (voorgestelde) oplossing is;
- contactgegevens voor de opvolging van de melding;
- aantal personen waarvan gegevens betrokken zijn bij de inbreuk (indien geen exact aantal bekend is: het minimale en maximale aantal personen waarvan gegevens betrokken zijn bij de inbreuk);
- een omschrijving van de groep personen van wie gegevens betrokken zijn bij de inbreuk;
- het soort of de soorten persoonsgegevens die betrokken zijn bij de inbreuk;
- de datum waarop de inbreuk heeft plaatsgevonden (indien geen exacte datum bekend is: de periode waarbinnen de inbreuk heeft plaatsgevonden);
- de datum en het tijdstip waarop de inbreuk bekend is geworden bij verwerker of bij een door hem ingeschakelde derde of onderaannemer;
- of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden;
- wat de reeds ondernomen maatregelen zijn om de inbreuk te beëindigen en om de gevolgen van de inbreuk te beperken.

## Bijlage 4: Subverwerkersregister Tribe CRM

Verwerker maakt bij de uitvoering van de overeenkomst gebruik van de subverwerkers die in deze bijlage zijn vermeld. De verwerker zal deze bijlage conform artikel 8 van de Tribe CRM verwerkersvoorwaarden van Efficacy Nederland B.V. bijwerken indien er wijzigingen plaatsvinden in de ingeschakelde subverwerkers en deze lijst onverwijld ter beschikking stellen aan de verwerkingsverantwoordelijke.

Voor de definitie van de gebruikte termen wordt verwezen naar de Tribe CRM verwerkersvoorwaarden van Efficacy Nederland B.V..

### Hosting

Subverwerker	<b>Google Ireland Limited</b>
Vestigingsplaats	Gordon House Barrow Street Dublin 4 Ireland
BTW nummer :	IE 6388047V
Beschrijving van de werkzaamheden	Hosting Tribe CRM platform waaronder redundante nutsvoorzieningen, infrastructuur opslagsystemen en (server-) hardware, toegangsbeveiliging, firewall en anti-DDos voorzieningen  <a href="https://cloud.google.com/security/infrastructure/">https://cloud.google.com/security/infrastructure/</a>
Certificeringen	<a href="https://cloud.google.com/security/compliance/#/">https://cloud.google.com/security/compliance/#/</a>

## E-mail providers

Subverwerker	<b>MailJet</b>
Vestigingsplaats	13 Rue De L Aubrac  75012 Parijs Frankrijk
BTW nummer :	FR67524536992
Beschrijving van de werkzaamheden	Mail aflevering systeem voor het versturen van berichten en de status terugkoppeling van de berichten van het Tribe CRM platform. Het scannen van uitgaande mailstromen op virus- en spamcontent.
Certificeringen	ISO 27001, <a href="https://www.mailjet.com/gdpr/mailjet-first-esp-iso-27001-and-gdpr-certified/">https://www.mailjet.com/gdpr/mailjet-first-esp-iso-27001-and-gdpr-certified/</a>  <a href="https://www.mailjet.com/privacy-policy/">https://www.mailjet.com/privacy-policy/</a>