Verwerkersovereenkomst

Versie 3.3, bijgewerkt 01-04-2026

Standaardcontractbepalingen (‘Standard contractual clauses’)

De partijen zijn het eens over de tekst van Implementatiebesluit (EU) 2021/915 van de Commissie van 4 juni 2021 betreffende standaardcontractbepalingen tussen voor de verwerkingsverantwoordelijken en verwerkers krachtens artikel 28, lid 7, van Verordening (EU) 2016/679 van het Europees Parlement en de Raad en artikel 29, lid 7, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad.

AFDELING I

Bepaling 1

Doel en toepassingsgebied

a) Het doel van deze standaardcontractbepalingen (hierna “de bepalingen” genoemd) is te zorgen voor de naleving van artikel 28, leden 3 en 4, van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

b) De in bijlage I vermelde verwerkingsverantwoordelijken en verwerkers hebben met deze bepalingen ingestemd teneinde te zorgen voor de naleving van artikel 28, leden 3 en 4, van Verordening (EU) 2016/679 en/of artikel 29, leden 3 en 4, van Verordening (EU) 2018/1725.

c) Deze bepalingen zijn van toepassing op de verwerking van persoonsgegevens als gespecificeerd in bijlage II.

d) De bijlagen I tot en met IV maken integrerend deel uit van de bepalingen.

e) Deze bepalingen laten de verplichtingen die op de verwerkingsverantwoordelijke rusten krachtens Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725 onverlet.

f) Deze bepalingen waarborgen op zichzelf niet de naleving van verplichtingen in verband met internationale doorgiften overeenkomstig hoofdstuk V van Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725.

Bepaling 2

Onveranderlijkheid van de bepalingen

a) De partijen verbinden zich ertoe de bepalingen niet te wijzigen, tenzij om informatie aan de bijlagen toe te voegen of de daarin vervatte informatie bij te werken.

b) Dit belet de partijen niet om de in deze bepalingen neergelegde standaardcontractbepalingen op te nemen in een bredere overeenkomst, of om andere bepalingen of aanvullende waarborgen toe te

voegen, mits deze niet direct of indirect in strijd zijn met de bepalingen of afbreuk doen aan de grondrechten of fundamentele vrijheden van betrokkenen.

Bepaling 3

Interpretatie

a) Wanneer in deze bepalingen de termen worden gebruikt die zijn gedefinieerd in Verordening (EU) 2016/679 respectievelijk Verordening (EU) 2018/1725, hebben die termen dezelfde betekenis als in die verordening.

b) Deze bepalingen moeten worden gelezen en geïnterpreteerd in het licht van de bepalingen van Verordening (EU) 2016/679 respectievelijk Verordening (EU) 2018/1725.

c) Deze bepalingen mogen niet worden geïnterpreteerd op een wijze die indruist tegen de rechten en verplichtingen waarin Verordening (EU) 2016/679/Verordening (EU) 2018/1725 voorziet of op een wijze die afbreuk doet aan de grondrechten of fundamentele vrijheden van de betrokkenen.

Bepaling 4

Hiërarchie

In geval van tegenstrijdigheid tussen deze standaardcontractbepalingen en de bepalingen van gerelateerde overeenkomsten tussen de partijen die reeds bestaan op het tijdstip waarop met deze standaardcontractbepalingen wordt ingestemd of die na dat tijdstip worden gesloten, prevaleren deze standaardcontractbepalingen.

Bepaling 5

Docking-bepaling

a) Elke entiteit die geen partij deze bepalingen is, kan, met instemming van alle partijen, te allen tijde tot deze bepalingen toetreden als verwerkingsverantwoordelijke of verwerker door de bijlagen in te vullen en bijlage I te ondertekenen.

b) Wanneer de in punt a) bedoelde bijlagen zijn ingevuld en ondertekend, wordt de toetredende partij als een partij bij deze bepalingen behandeld en heeft zij de rechten en verplichtingen van een verwerkingsverantwoordelijke of verwerker, al naar gelang zij in bijlage I is aangeduid.

c) Voor de toetredende entiteit vloeien uit deze bepalingen geen rechten of verplichtingen voort met betrekking tot de periode voordat zij partij werd.

AFDELING II

VERPLICHTINGEN VAN PARTIJEN

Bepaling 6

Beschrijving van de verwerking(en)

De bijzonderheden van de verwerkingen, en met name de categorieën persoonsgegevens en de doeleinden van de verwerking waarvoor de persoonsgegevens namens de verwerkingsverantwoordelijke worden verwerkt, zijn gespecificeerd in bijlage II.

Bepaling 7

Verplichtingen van de partijen

7.1. **Instructies**

a) De verwerker verwerkt persoonsgegevens uitsluitend op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, tenzij een op de verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht. In dat geval stelt de verwerker de verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij de wetgeving dit om gewichtige redenen van algemeen belang verbiedt. De verwerkingsverantwoordelijke kan ook tijdens de verwerking van persoonsgegevens steeds verdere instructies geven. Deze instructies worden altijd schriftelijk vastgelegd.

b) De verwerker stelt de verwerkingsverantwoordelijke onmiddellijk in kennis als de instructies van de verwerkingsverantwoordelijke naar het oordeel van de verwerker inbreuk maken op Verordening (EU) 2016/679/Verordening (EU) 2018/1725 of de toepasselijke gegevensbeschermingsbepalingen van de Unie of de lidstaten.

7.2. **Doelbinding**

De verwerker verwerkt de persoonsgegevens uitsluitend voor het specifieke doel of de specifieke doeleinden van de verwerking, zoals beschreven in bijlage II, tenzij hij verdere instructies van de verwerkingsverantwoordelijke krijgt.

7.3. **Doel van de verwerking van persoonsgegevens**

Verwerking door de verwerker vindt slechts plaats gedurende de in bijlage II vastgestelde tijdspanne.

7.4. **Beveiliging van de verwerking**

a) De verwerker treft ten minste de in bijlage III gespecificeerde technische en organisatorische maatregelen om de beveiliging van de persoonsgegevens te waarborgen. Dit houdt onder meer in dat de gegevens worden beschermd tegen een inbreuk op de beveiliging die leidt tot de vernietiging, het

verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot de gegevens, hetzij per ongeluk hetzij onrechtmatig (inbreuk in verband met persoonsgegevens). Bij de beoordeling van het passende beveiligingsniveau houden de partijen naar behoren rekening met de stand van de techniek, de uitvoeringskosten, de aard, de reikwijdte, de context en de doeleinden van de verwerking en de risico's voor de betrokkenen.

b) De verwerker verleent zijn personeel slechts toegang tot de persoonsgegevens die worden verwerkt voor zover dat strikt noodzakelijk is voor de uitvoering, het beheer en de monitoring van de overeenkomst. De verwerker waarborgt dat de tot het verwerken van de ontvangen persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden.

7.5. **Gevoelige gegevens**

Indien de verwerking betrekking heeft op persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, of betrekking heeft op genetische gegevens of biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (hierna "gevoelige gegevens" genoemd), voorziet de verwerker in specifieke beperkingen en/of aanvullende waarborgen.

7.6. **Documentatie en naleving**

a) De partijen kunnen aantonen dat aan deze bepalingen is voldaan.

b) De verwerker behandelt verzoeken van de verwerkingsverantwoordelijke inzake de verwerking van gegevens overeenkomstig deze bepalingen onverwijld en adequaat.

c) De verwerker stelt de verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om aan te tonen dat is voldaan aan de in deze bepalingen vastgestelde verplichtingen die rechtstreeks voortvloeien uit Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725. Op verzoek van de verwerkingsverantwoordelijke staat de verwerker ook regelmatig, of indien er aanwijzingen van niet-naleving zijn, audits toe van de onder deze bepalingen vallende verwerkingsactiviteiten en draagt de verwerker aan die audits bij. Bij het nemen van een beslissing over een toetsing of audit kan de verwerkingsverantwoordelijke rekening houden met relevante certificeringen van de verwerker.

d) De verwerkingsverantwoordelijke kan ervoor kiezen de audit zelf uit te voeren of een onafhankelijke auditor daartoe opdracht te geven. De audits kunnen ook inspecties in de bedrijfsruimten of fysieke faciliteiten van de verwerker omvatten en worden, in voorkomend geval, tijdig aangekondigd.

e) De partijen stellen de in deze bepaling bedoelde informatie, met inbegrip van de resultaten van eventuele audits, op verzoek ter beschikking van de bevoegde toezichthoudende autoriteit/autoriteiten.

7.7. **Gebruik van subverwerkers**

a) ALGEMENE SCHRIFTELIJKE TOESTEMMING: De verwerker heeft de algemene toestemming van de verwerkingsverantwoordelijke om subverwerkers in dienst te nemen die op een overeengekomen lijst staan. De verwerker stelt de verwerkingsverantwoordelijke ten minste 14 kalender dagen van tevoren specifiek schriftelijk in kennis van voorgenomen wijzigingen van die lijst door toevoeging of

vervanging van subverwerkers, zodat de verwerkingsverantwoordelijke voldoende tijd heeft om vóór de indienstneming van de betrokken subverwerker(s) bezwaar te kunnen maken tegen dergelijke wijzigingen. De verwerker verstrekt de verwerkingsverantwoordelijke de informatie die nodig is om deze laatste in staat te stellen zijn recht van bezwaar uit te oefenen.

b) Wanneer de verwerker een subverwerker in dienst neemt voor de uitvoering van specifieke verwerkingen (namens de verwerkingsverantwoordelijke), doet hij dit door middel van een overeenkomst die de subverwerker in wezen dezelfde verplichtingen inzake gegevensbescherming oplegt als die welke op grond van deze bepalingen aan de verwerker worden opgelegd. De verwerker zorgt ervoor dat de subverwerker voldoet aan de verplichtingen die krachtens deze bepalingen en Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725 op de verwerker rusten.

c) Op verzoek van de verwerkingsverantwoordelijke verstrekt de verwerker de verwerkingsverantwoordelijke een kopie van een dergelijke subverwerkingsovereenkomst en van alle latere wijzigingen daarvan. Voor zover nodig ter bescherming van bedrijfsgeheimen of andere vertrouwelijke informatie, met inbegrip van persoonsgegevens, kan de verwerker de tekst van de overeenkomst bewerken alvorens de kopie te delen.

d) De verwerker blijft ten opzichte van de verwerkingsverantwoordelijke volledig verantwoordelijk voor de uitvoering van de verplichtingen van de subverwerker overeenkomstig zijn overeenkomst met de verwerker. De verwerker stelt de verwerkingsverantwoordelijke in kennis van elk verzuim van de subverwerker om zijn contractuele verplichtingen na te komen.

e) De verwerker komt met de subverwerker een derdenbeding overeen waarbij — ingeval de verwerker feitelijk is verdwenen, rechtens is opgehouden te bestaan of insolvent is geworden — de verwerkingsverantwoordelijke het recht heeft de overeenkomst met de subverwerker te beëindigen en de subverwerker te gelasten de persoonsgegevens te wissen of terug te geven.

7.8. **Internationale doorgiften**

a) Doorgifte van gegevens aan een derde land of een internationale organisatie door de verwerker geschiedt uitsluitend op basis van schriftelijke instructies van de verwerkingsverantwoordelijke of om te voldoen aan een specifieke eis uit hoofde van het Unierecht of het lidstatelijke recht waaraan de verwerker is onderworpen, en vindt plaats in overeenstemming met hoofdstuk V van Verordening (EU) 2016/679 of Verordening (EU) 2018/1725.

b) De verwerkingsverantwoordelijke stemt ermee in dat wanneer de verwerker overeenkomstig bepaling 7.7 een subverwerker in dienst neemt voor het uitvoeren van specifieke verwerkingen (namens de verwerkingsverantwoordelijke) en die verwerkingen een doorgifte van persoonsgegevens in de zin van hoofdstuk V van Verordening (EU) 2016/679 inhouden, de verwerker en de subverwerker de naleving van hoofdstuk V van Verordening (EU) 2016/679 kunnen waarborgen door gebruik te maken van standaardcontractbepalingen die door de Commissie zijn vastgesteld overeenkomstig artikel 46, lid 2, van Verordening (EU) 2016/679, mits aan de voorwaarden voor het gebruik van die standaardcontractbepalingen is voldaan.

Bepaling 8

Bijstand aan de verwerkingsverantwoordelijke

a) De verwerker stelt de verwerkingsverantwoordelijke onverwijld in kennis van elk verzoek dat hij van de betrokkene heeft ontvangen. De verwerker antwoordt niet zelf op het verzoek, tenzij de verwerkingsverantwoordelijke daartoe toestemming heeft gegeven.

b) De verwerker staat de verwerkingsverantwoordelijke bij bij het vervullen van zijn verplichtingen om te reageren op verzoeken van betrokkenen tot uitoefening van hun rechten, en houdt daarbij rekening met de aard van de verwerking. Bij het nakomen van zijn verplichtingen uit hoofde van de punten a) en b) volgt de verwerker de instructies van de verwerkingsverantwoordelijke.

c) De verwerker heeft niet alleen de verplichting de verwerkingsverantwoordelijke bij te staan overeenkomstig bepaling 8, punt b), maar staat de verwerkingsverantwoordelijke ook bij bij het waarborgen van de naleving van de volgende verplichtingen, waarbij rekening wordt gehouden met de aard van de gegevensverwerking en de informatie waarover de verwerker beschikt:

1) de verplichting om een beoordeling uit te voeren van het effect van de beoogde verwerkingen op de bescherming van persoonsgegevens (een “gegevensbeschermingseffectbeoordeling”) wanneer een bepaalde soort verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen;

2) de verplichting om de bevoegde toezichthoudende autoriteit/autoriteiten voorafgaand aan de verwerking te raadplegen wanneer uit een gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om dat risico te beperken;

3) de verplichting om ervoor te zorgen dat persoonsgegevens accuraat en actueel zijn, door de verwerkingsverantwoordelijke onverwijld in te lichten wanneer de verwerker ervan kennis heeft gekregen dat de gegevens die hij verwerkt onjuist of achterhaald zijn;

4) de verplichtingen in artikel 32 van Verordening (EU) 2016/679.

d) De partijen stellen in bijlage III de passende technische en organisatorische maatregelen vast op grond waarvan de verwerker de verwerkingsverantwoordelijke bij de toepassing van deze bepaling moet bijstaan, alsmede de omvang en de omvang van de vereiste bijstand.

Bepaling 9

Kennisgeving van een inbreuk in verband met persoonsgegevens

In het geval van een inbreuk in verband met persoonsgegevens werkt de verwerker samen met de verwerkingsverantwoordelijke en staat hij hem bij opdat de verwerkingsverantwoordelijke kan voldoen aan zijn verplichtingen uit hoofde van de artikelen 33 en 34 van Verordening (EU) 2016/679 of de artikelen 34 en 35 van Verordening (EU) 2018/1725, indien van toepassing, waarbij rekening wordt gehouden met de aard van de verwerking en de informatie waarover de verwerker beschikt.

9.1. **Inbreuk in verband met gegevens die door de verwerkingsverantwoordelijke worden verwerkt**

SoSafe SE

In geval van een inbreuk in verband met persoonsgegevens die door de verwerkingsverantwoordelijke worden verwerkt, staat de verwerker de verwerkingsverantwoordelijke bij:

a) bij het zonder onnodige vertraging melden van de inbreuk in verband met persoonsgegevens aan de bevoegde toezichthoudende autoriteit/autoriteiten nadat de verwerkingsverantwoordelijke er kennis van heeft gekregen, indien relevant /(tenzij het onwaarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen);

b) bij het verkrijgen van onderstaande informatie die overeenkomstig artikel 33, lid 3, van Verordening (EU) 2016/679in de kennisgeving van de verwerkingsverantwoordelijke moet worden vermeld en ten minste omvat:

1) de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;

2) de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;

3) de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Indien en voor zover al deze informatie niet op hetzelfde moment kan worden verstrekt, bevat de oorspronkelijke kennisgeving de dan beschikbare informatie en wordt verdere informatie vervolgens onverwijld verstrekt zodra deze beschikbaar is;

c) bij het naleven, overeenkomstig artikel 34 van Verordening (EU) 2016/679, van de verplichting om de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee te delen, wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

9.2. **Inbreuk in verband met gegevens die door de verwerker worden verwerkt**

In geval van een inbreuk in verband met persoonsgegevens die door de verwerker worden verwerkt, stelt de verwerker, nadat hij kennis heeft gekregen van de inbreuk, de verwerkingsverantwoordelijke daarvan onverwijld in kennis. Deze kennisgeving bevat ten minste:

a) een beschrijving van de aard van de inbreuk (waar mogelijk onder vermelding van de categorieën betrokkenen en gegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en gegevensregisters in kwestie);

b) de gegevens van een contactpunt waar meer informatie over de inbreuk in verband met persoonsgegevens kan worden verkregen;

c) de waarschijnlijke gevolgen van de inbreuk en de maatregelen die zijn genomen of worden voorgesteld om deze aan te pakken, onder meer om de mogelijke negatieve gevolgen ervan te beperken.

Indien en voor zover al deze informatie niet op hetzelfde moment kan worden verstrekt, bevat de oorspronkelijke kennisgeving de dan beschikbare informatie en wordt verdere informatie vervolgens onverwijld verstrekt zodra deze beschikbaar is.

De partijen vermelden in bijlage III alle andere elementen die door de verwerker moeten worden verstrekt wanneer hij de verwerkingsverantwoordelijke bijstaat bij de naleving van de verplichtingen van de verwerkingsverantwoordelijke uit hoofde van de [OPTIE 1] de artikelen 33 en 34 van Verordening (EU) 2016/679/[OPTIE 2] de artikelen 34 en 35 van Verordening (EU) 2018/1725.

AFDELING III

SLOTBEPALINGEN

Bepaling 10

Niet-naleving van de bepalingen en beëindiging

a) Onverminderd eventuele bepalingen van Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725 kan de verwerkingsverantwoordelijke, ingeval de verwerker zijn verplichtingen uit hoofde van deze bepalingen niet nakomt, de verwerker opdracht geven de verwerking van persoonsgegevens op te schorten totdat deze aan deze bepalingen voldoet of de overeenkomst wordt beëindigd. Wanneer de verwerker om welke reden dan ook niet aan deze bepalingen kan voldoen, stelt hij de verwerkingsverantwoordelijke daarvan onverwijld in kennis.

b) De verwerkingsverantwoordelijke heeft het recht de overeenkomst te beëindigen voor zover deze de verwerking van persoonsgegevens overeenkomstig deze bepalingen betreft, indien:

1) de verwerkingsverantwoordelijke de verwerking van persoonsgegevens door de verwerker overeenkomstig punt a) heeft opgeschort en de naleving van deze bepalingen niet binnen een redelijke termijn en in elk geval binnen één maand na de opschorting wordt hervat;

2) de verwerker deze bepalingen of zijn verplichtingen uit hoofde van Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725 wezenlijk of voortdurend schendt;

3) de verwerker niet voldoet aan een bindend besluit van een bevoegde rechter of de bevoegde toezichthoudende autoriteit/autoriteiten met betrekking tot zijn verplichtingen uit hoofde van deze bepalingen of Verordening (EU) 2016/679 en/of Verordening (EU) 2018/1725.

c) De verwerker heeft het recht de overeenkomst op te zeggen voor zover het daarbij gaat om de verwerking van persoonsgegevens krachtens deze bepalingen, indien de verwerkingsverantwoordelijke, nadat de verwerker hem er overeenkomstig bepaling 7.1, punt b), van in kennis heeft gesteld dat zijn instructies inbreuk maken op de toepasselijke wettelijke vereisten, aandringt op naleving van de instructies.

d) Na de beëindiging van de overeenkomst wist de verwerker, naar keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens die namens de verwerkingsverantwoordelijke zijn verwerkt en bevestigt hij tegenover de verwerkingsverantwoordelijke dat hij dit heeft gedaan, of zendt hij alle persoonsgegevens terug aan de verwerkingsverantwoordelijke en verwijdert hij bestaande

kopieën, tenzij het Unierecht of het lidstatelijke recht de opslag van de persoonsgegevens voorschrijft. Totdat de gegevens zijn gewist of teruggeven, blijft de verwerker ervoor zorgen dat deze bepalingen worden nageleefd.

BIJLAGE I – Lijst van partijen

Verwerkingsverantwoordelijk(en):

De contactpersoon die de Klant na ondertekening van het hoofdcontract in de SoSafe Manager heeft aangewezen, is de primaire ontvanger van de communicatie.

Meldingen worden uiterlijk bij de aanvang van de implementatie van de Awareness Diensten doorgestuurd naar de Beheerder van de Klant zoals aangegeven in de SoSafe Manager, totdat een contactpersoon is aangewezen door de Klant.

Verwerker(s)

SoSafe SE
Lichtstr. 25a
50825 Köln

Functionaris gegevensbescherming :

Mr. Sebastian Herting
Herting Oberbeck Datenschutz GmbH
Hallerstraße 76
20146 Hamburg
E-Mail: dpo@sosafe.de

Opmerking: een kopie van de communicatie die naar de Functionaris gegevensbescherming wordt gestuurd, ontvangt SoSafe ook graag via privacy@sosafe.de.

BIJLAGE II – Beschrijving van de verwerking

1. Doel

De diensten van Verwerker die de basis vormen voor de verwerkingsactiviteiten van de Verwerker op grond van deze Verwerkersovereenkomst zijn in detail gespecificeerd in de Hoofdovereenkomst. De verwerking van persoonsgegevens in opdracht van de Verwerkingsverantwoordelijke in het kader van deze Verwerkersovereenkomst heeft specifiek betrekking op het volgende:

Levering van een Software-as-a-Service platform voor human risk management, training en gebruikerstesten. Afhankelijk van de keuze van de Verwerkingsverantwoordelijke voor afzonderlijke SoSafe Awareness Diensten, krijgen Gebruikers van de Verwerkingsverantwoordelijke of zijn Gelieerde Ondernemingen onder de Hoofdovereenkomst toegang tot social engineering-simulaties (bijv. phishing, smishing, vishing), vragenlijsten, tests, optionele AI-gestuurde chatbots en tooling en andere gebruikersgerichte risicoprofielmechanismen. Veiligheidsbewustzijnstrainingen, analyses, feedbackmechanismen en technische en procedurele interventies kunnen automatisch of handmatig worden geactiveerd, zoals geconfigureerd door de Verwerkingsverantwoordelijke, of anderszins worden geleverd als gevolg van gebruikersinteractie met het Platform of gegevens die door het Platform worden opgenomen via technische integraties met andere bedrijfssystemen van de Verwerkingsverantwoordelijke, zoals geïmplementeerd of anderszins gespecificeerd door de Verwerkingsverantwoordelijke.

Het Platform kan een gepersonaliseerd profiel van een Gebruiker creëeren en geautomatiseerde acties uitvoeren om het veilige gedrag van de Gebruiker te rapporteren of te verbeteren, met inachtneming van de door de Verwerkingsverantwoordelijke gekozen anonimiseringsinstellingen.

2. Duur

De duur van de verwerking door Verwerker is afhankelijk van de duur van de Hoofdovereenkomst. De verwerking en deze Overeenkomst inzake opdracht specifieke verwerking eindigen dus wanneer de Hoofdovereenkomst (plus de toepasselijke opslagperiode na beëindiging van het contract in overeenstemming met het verwijderingsbeleid) eindigt, voor zover er geen blijvende verplichtingen voortvloeien uit de voorwaarden van deze Overeenkomst inzake opdrachtspecifieke verwerking of deze Overeenkomst niet voortijdig wordt beëindigd.

3. Doel van de verwerking

De verwerking dient het volgende doel: de Verwerkingsverantwoordelijke moet in staat worden gesteld de door de Verwerker aangeschafte Awareness Diensten aan Gebruikers te verlenen.

4. Categorieën van persoonsgegevens

De volgende soorten persoonsgegevens, alle met betrekking tot Gebruikers, worden verwerkt door Verwerker namens de Verwerkingsverantwoordelijke in het kader van het leveren van de Awareness Diensten zoals nader gespecificeerd in de Hoofdovereenkomst.

(1) Gegevens voor registratie en accountbeheer

SoSafe SE

Alle Awareness Diensten verwerken bepaalde soorten gegevens die worden gevraagd van gebruikers om zich te registreren voor de Awareness Diensten en om de Awareness Diensten en het account te beheren namens de Verwerkingsverantwoordelijke ("Gegevens voor registratie en accountbeheer"), waaronder met name:

- Voor- en achternaam
- Werk e-mailadres
- Toegewezen gebruikersgroepen (bijv. organisatie-eenheid, locatie, rol), toegangsniveaus
- *Optionele* gebruikersvoorkeuren, zoals aanhef en taal

(2) Gebruiksgegevens

Naast Gegevens voor registratie en accountbeheer kunnen, afhankelijk van de gekozen Awareness Diensten, andere gegevenstypen met betrekking tot Gebruikers worden verwerkt om de Awareness Diensten uit te voeren en te leveren, zoals nader gespecificeerd in het Hoofdcontract:

- Informatie over de scoping en afstemming van de Gebruiker, zoals rol, afdeling, kennisniveau bij aanvang van het gebruik van de Awareness Diensten, antwoorden op inleidende vragenlijsten;
- Gebruikersactiviteit op het platform, zoals het starten en afronden van trainingen, testscores, interactie met testen;
- Escalatie-informatie (bijv. relaties met lijnmanagers);
- Optionele AI-modules: interactie met AI-gestuurde chatbots en tooling voor zover deze persoonsgegevens bevatten op basis van de input die de Verwerker ontvangt van de Gebruiker van de AI-module door de Verwerkingsverantwoordelijke;
- Optionele PhishFeedback-module: regio-instellingen van de gebruiker (bijv. taal en tijdzone) en gerapporteerde e-mail, waarbij zowel de regio-instellingen als de gerapporteerde email persoonlijke gegevens kunnen bevatten.

(3) Technische gegevens

Gegevens met betrekking tot Gebruikers die nodig zijn voor de werking van de applicatie en de infrastructuur en die nodig zijn voor het voldoen aan de verplichtingen van onze Technische en organisatorische maatregelen, waaronder met name:

- Systeeminformatie van de gebruiker die vereist is door de applicatie, zoals browserversie en -platform, informatie over de gebruikersagent;
- Netwerkgegevens zoals IP-adres, tijdstempel, URL en API-eindpunten waartoe toegang is verkregen;
- Mailgegevens zoals adressen van afzenders en ontvangers, routeringsinformatie en tijdstempels;
- Gegevens verzameld uit integraties die zijn aangevraagd of geïmplementeerd door de Verwerkingsverantwoordelijke en die organisatie- of gebruikersgegevens kunnen bevatten, zoals waarschuwingen van DLP-tooling (Data Loss Prevention), endpointdetectie en responsagenten.

5. Categorieën van betrokkenen

De betrokkenen zijn, tenzij in de Hoofdovereenkomst anders is bepaald, alle gebruikers die door de verwerkingsverantwoordelijke voor deelname zijn opgegeven. Het staat de

verwerkingsverantwoordelijke vrij om niet-deelname voor individuele gebruikers mogelijk te maken via een opt-out proces.

BIJLAGE III – Technische en organisatorische maatregelen, met inbegrip van technische en organisatorische maatregelen om de beveiliging van de gegevens te waarborgen

De technische en organisatorische maatregelen ter waarborging van de gegevensbescherming en -beveiliging, die de Verwerker ten minste moet treffen en continu handhaven, worden hieronder gedefinieerd. Het doel is in het bijzonder het garanderen van vertrouwelijkheid, integriteit en beschikbaarheid van de informatie die het onderwerp is van orderspecifieke verwerkingen.

1. Configureerbare anonimisering en doelgerichte toegang tot gegevens

Alle diensten van de Verwerker kunnen zodanig worden geconfigureerd dat Beheerders van Klanten standaard alleen geanonimiseerde geaggregeerde toegang hebben tot gebruikersgegevens. Toegang voor specifiek personeel van de Verwerkingsverantwoordelijke op individueel niveau kan worden geconfigureerd wanneer de Verwerkingsverantwoordelijke dit duidelijk en expliciet verzoekt.

2. Encryptie

2.1 Gegevens in transit

Alle gegevensuitwisselingen (tussen zowel de Verwerkingsverantwoordelijke en de Verwerker als tussen alle medewerkers van de Verwerker) worden sterk versleuteld in overeenstemming met de goede praktijken in de branche, zoals ECC met Curve25519, RSA met een sleutel van 2048 bits of langer, bijgewerkt volgens de laatste stand van de techniek. De interne netwerktoegang en administratieve toegang van SoSafe is sterk versleuteld. Voor communicatie met service-eindpunten is een beveiligde verbinding nodig.

2.2 Gegevens in rust

Alle persoonlijk identificeerbare gegevens van de Verwerkingsverantwoordelijke en Gebruikersgegevens worden door het Platform op gepaste wijze versleuteld op het opslagniveau met behulp van krachtige algoritmen en implementaties die in de industrie als goed worden beschouwd, zoals AES-256-GCM of beter.

2.3 Gegevens in gebruik

De oplossing van de Verwerker betreft een pure cloudapplicatie waarmee de front-end op de computer van de eindgebruiker wordt bediend. Dit biedt geen mogelijkheid tot encryptie.

3. Vertrouwelijkheid

3.1 Fysieke toegangscontrole

De kantoorruimtes van de Verwerker zijn alleen toegankelijk met de betreffende sleutels of transponders met bijbehorende veiligheidssloten. De uitgifte van sleutels en transponders wordt gedocumenteerd en medeondertekend door het management van de Verwerker. Passende inbraakalarmen, CCTV-dekking en reactieprocedures zijn aanwezig. SoSafe-kantoren bieden geen speciale toegangsrechten tot het netwerk, behalve toegang tot het internet.

Het SoSafe-platform wordt gehost door toonaangevende hyperscale Cloud Service Providers. Deze providers werken vanuit datacenters die de juiste fysieke en omgevingscontroles implementeren. Deze controles omvatten, maar zijn niet beperkt tot:

- Het volgen en bewaken van alle toegang van bezoekers en personeelsbewegingen
- CCTV-bewaking met een bewaarperiode van 90 dagen
- Sterke toegangscontrole tot alle datahosting-, netwerk-, machine- en omgevingsruimten
- Ten minste N+1 redundantie van stroom-, netwerk- en omgevingsdiensten

Aanbieders van clouddiensten moeten een ISO 27001- en/of SOC2-accreditatie of een vergelijkbare accreditatie hebben. SoSafe beoordeelt hun fysieke beveiliging door audit- en accreditatiemateriaal te beoordelen.

3.2 Logisch toegangsbeheer

Alle logische toegang vereist een multi-factor geverifieerde VPN-verbinding. De kantoornetwerken geven geen speciale netwerkrechten behalve toegang tot het internet. Authenticatie voor de bedrijfssystemen van SoSafe vindt plaats via SSO waarbij multifactorauthenticatie en sterke, beleidsgedefinieerde wachtwoorden vereist zijn, in overeenstemming met de goede praktijken in de sector. Alle systeemtoegang, inclusief toegang tot klantgegevens, wordt uitsluitend verleend op een controleerbare, gedetailleerd omschreven 'need-to-know'-basis. De toegangsrechten van interne gebruikers worden regelmatig herzien.

3.3 Beveiliging van eindpunten

Alle apparaten van eindgebruikers worden veilig geconfigureerd door Mobile Device Management waarbij alle controles worden afgedwongen en gebruik wordt gemaakt van Endpoint Detection and Response-agents. Er is volledige schijfversleuteling aanwezig. Apparaten van eindgebruikers worden na maximaal vijf (5) minuten inactiviteit uitgeschakeld. Alle apparaten van eindgebruikers beschikken over individuele antivirus- en firewallsoftware met een automatische updatefunctie. Updates van besturingssystemen en belangrijke softwarepakketten worden op de juiste manier beheerd.

3.4 Controle op het doorsturen

Het gegevensverkeer met persoonlijke informatie wordt geminimaliseerd en beperkt tot de mate die nodig is om de dienst te verlenen. Aan de kant van de Verwerker heeft alleen het personeel waarvoor toegang tot persoonlijke informatie relevant en noodzakelijk is, toegang tot deze informatie (op een “need-to-know” basis).

Er is een beleid voor werken op afstand en er zijn passende controles. Persoonlijke gegevens mogen niet worden opgeslagen op apparaten van eindgebruikers. Alle medewerkers zijn contractueel verplicht tot geheimhouding en bescherming van bedrijfsgeheimen.

Er is een Bring Your Own Device (BYOD)-risicobeoordeling is uitgevoerd in het kader van ISO 27001 en er is relevant beleid om het gebruik en de risico's van BYOD te beperken. Passende centraal beheerde controles zijn aanwezig.

3.5 Verwijderen van gegevens

De leveranciers van clouddiensten die door de Verwerker worden gebruikt, zorgen voor logische gegevensvernietiging in overeenstemming met erkende industrieprocedures.

Systeemlogboeken en beveiligingsgegevens kunnen tot 12 maanden na de datum van aanmaak worden bewaard om passende reacties op beveiligingsincidenten en forensisch onderzoek mogelijk te maken. Systeemback-ups worden adequaat beschermd en alle gebruikersgegevens daarin worden binnen 12 maanden na aanmaak verwijderd in overeenstemming met het back-upbeleid van de Verwerker.

3.6 Scheidingscontrole

Er is een scheiding tussen productieve, test-/ontwikkelings- en beheersystemen. Er zijn databaserechten gedefinieerd en er is een logische scheiding van systemen in de software, afgedwongen door databaselogica.

4. Integriteit

Toegang tot de databases van de productieve systemen wordt vastgelegd en twaalf (12) maanden bewaard. Er zijn passende back-up- en herstelprocedures om de integriteit van gegevens te beschermen. Toegang tot de database is beperkt op basis van rollen.

5. Beschikbaarheid

5.1 Bedrijfscontinuïteit

De productsystemen en servers worden continu gemonitord door de Verwerker om een constante beschikbaarheid te garanderen. Verwerker hanteert een adequaat architectuur- en bedrijfscontinuïteitssysteem als onderdeel van de ISO 27001-audit en accreditatie, voldoende om te voldoen aan de SLA's gedefinieerd in de Hoofdovereenkomst. Van de servers en productsystemen wordt dagelijks continu een back-up gemaakt. De back-ups worden versleuteld en opgeslagen op aparte serversystemen van de Verwerker. Toegang wordt alleen verleend aan de beheerders van de Verwerker.

5.2 Veiligheidsbewustzijn en -training

Alle medewerkers van de Verwerker worden voortdurend en uitgebreid getraind (seminars, e-learning en interactieve formats zoals quizzen) op het gebied van gegevensbescherming en fundamentele onderwerpen met betrekking tot informatiebeveiliging.

6. Incident Management

De Verwerker hanteert passende maatregelen op het gebied van beveiligingsmonitoring, incidentdetectie en -respons, waaronder technische logboekregistratie en geautomatiseerde auditcontroles, een Security Operations-team en -capaciteit en organisatiebrede incidentresponsprocessen. Alle significante beveiligingsincidenten, inclusief bijna-incidenten, vereisen een formele retrospectieve en analyse van de hoofdoorzaak.

7. Information Security Management System

Verwerker hanteert een formeel Information Security Management System (ISMS) volgens de vereisten van ISO 27001 en wordt extern geauditeerd en geaccrediteerd in overeenstemming met deze vereisten. Verwerker verkrijgt ook andere branche-accreditaties zoals TISAX indien vereist. Formele beleidslijnen en procedures voor risicobeoordeling en -beheer worden uitgevoerd door de Security-organisatie, met regelmatige, geplande input en rapportering aan het Security Comité, dat bestaat uit relevante leden van het Security- en Executive Team. Het ISMS wordt formeel ondersteund door het Executive Team en de CEO.

Het ISMS en alle beveiligingsfuncties worden uitgevoerd door een Security-organisatie met de benodigde middelen onder leiding van een Chief Information Security Officer.

8. Regelmatige beoordeling van technische en organisatorische maatregelen

Alle relevante beveiligings-, privacy- en operationele processen worden jaarlijks intern geaudit door deskundige, gekwalificeerde auditors, met input in het ISMS en het Security Comité. Het ISMS van de Verwerker wordt ten minste eenmaal per jaar formeel extern geaudit door een erkend professioneel bedrijf.

BIJLAGE IV – Lijst van Subverwerkers

Ga naar https://sosafe-awareness.com/nl/legal/sub-processors/voor een actuele lijst van subverwerkers, verwerkingsactiviteiten en waarborgen.