Verwerkersovereenkomst

Versie 3.0, bijgewerkt 13.12.2023

SoSafe GmbH | Lichtstr. 25a | 50825 Cologne | sosafe.de

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**

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(n):

[Identiteit en contactgegevens van de verwerkingsverantwoordelijke(n) en, in voorkomend geval, van de functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke]

Naam: Vul hier de naam van de verwerkingsverantwoordelijke in

Adres: Vul hier het adres van de verwerkingsverantwoordelijke in

Naam, functie en contactgegevens van de contactpersoon:
Vul hier de naam, functie en contactgegevens van de contactpersoon van de verwerkingsverantwoordelijke in

Ondertekening en toetredingsdatum:

Verwerker(s)

SoSafe GmbH
Lichtstr. 25a
50825 Köln

Functionaris voor gegevensbescherming :

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

Felix Schürholz, Managing Director

Ondertekening en toetredingsdatum:

DocuSigned by:
Felix Schürholz
6459695B96B249C...

22 April 2024 | 08:37 PDT

BIJLAGE II – Beschrijving van de verwerking

1. Doel

In het kader van zijn dienstverlening verricht de Opdrachtnemer met name die activiteiten waarvoor persoonsgegevens worden verwerkt (een volledige lijst staat in de Hoofdovereenkomst):

(1) Uitvoering van anonieme Phishing simulaties

Het versturen van phishing mails:

- Op basis van de door de Opdrachtgever verstrekte e-mailadressen en namen van werknemers (in het hiernavolgende: de "Gebruikers") verstuurt de Opdrachtnemer gedurende een bepaalde periode een bepaald aantal e-mailtemplates.
- De e-mailtemplates zijn gepersonaliseerd, dat wil zeggen dat zij een persoonlijk adres met de respectieve naam van de gebruiker bevatten om een realistische phishing aanval te simuleren.
- Indien gewenst door de Opdrachtgever kan deze dienst op een meer genuanceerde wijze worden verleend met aanvullende categorisatiecriteria (bijvoorbeeld organisatie-eenheid, locatie, status als lid van de directie). De groepen ontvangers/gebruikers die uit deze indelingscriteria voortvloeien, moeten echter altijd uit ten minste vijf (5) personen bestaan.
- Elke individuele e-mail bevat ook een identieke link naar een onzichtbaar afbeeldingsbestand (tracking pixel) dat wordt gedownload wanneer de e-mail wordt geopend.

Feedback aan gebruikers bij gebruik van trainingspagina's via browser:

- De e-mailtemplates bevatten elk een unieke, template-specifieke link (zij het identiek voor alle gebruikers van de Opdrachtgever) die leidt naar een trainingspagina die wordt gehost op een webserver van de Opdrachtnemer.
- Wanneer de gebruikers op de link klikken, worden zij naar de trainingspagina geleid en wordt de desbetreffende e-mail (zonder gepersonaliseerd adres) getoond met een uitleg over hoe deze kan worden herkend als een phishing mail.

Gebruik van de Phishing Report Button:

- Optioneel kan een add-on voor diverse e-mailprogramma's (zoals Microsoft Outlook) worden geïnstalleerd, waarmee gebruikers verdachte e-mails kunnen melden. Indien de betreffende e-mail van de simulatie afkomstig is, wordt de klik meegerekend in het rapportagepercentage van de evaluatie, dat op zijn beurt door de Opdrachtnemer wordt geregistreerd. Opgenomen gegevens worden geanonimiseerd en alleen geanonimiseerde gegevens worden naar de Opdrachtgever gestuurd. In dit geval wordt geen feedback of gegevensstroom naar de Opdrachtnemer gestuurd.

(2) Terbeschikkingstelling van een e-learning trainingsplatform:

- Gebruikers kunnen zich voor het e-learning trainingsportaal op het platform van de Opdrachtnemer registreren met hun werk e-mailadres op https://elearning.sosafe.de/registration en toegang krijgen tot alle voor hen beschikbare of door de Opdrachtgever verstrekte e-learning modules. In elke module kan een korte quiz worden gedaan. Op basis van de antwoorden wordt een resultaat bepaald (op basis van het aantal juiste antwoorden). Deze quiz kan onbeperkt herhaald worden.
- De e-learning trainingsmodules kunnen ook als SCORM-bestanden aan de Opdrachtgever worden verstrekt om de integratie in een bestaand learning management systeem te bevorderen.

(3) Terbeschikkingstelling van een evaluatie (Reporting Dashboard):

- De open-, antwoord-, invoer- en klikpercentages (algemeen en per gedefinieerde groepering volgens categoriale criteria, zie punt 1.1 (1)) kunnen worden bepaald op basis van het totale aantal verzonden e-mails. Deze informatie wordt aan de Opdrachtgever verstrekt via een evaluatieportaal. Gepersonaliseerde tracering is echter niet mogelijk omdat elke organisatorische eenheid uit ten minste vijf (5) personen moet bestaan.
- Indien het trainingsplatform van de Opdrachtnemer wordt gebruikt voor e-learning, worden het aantal inschrijvingen, de modulevoortgang en de resultaten van de e-learning trainingsquizzen geregistreerd voor de individuele gebruikers en (tenzij anders overeengekomen) gerapporteerd aan de Opdrachtgever.
- Bij gebruik van de Phishing Report Button wordt ook de totale en gecategoriseerde report rate (d.w.z. hoeveel e-mails van de simulatie door gebruikers zijn geïdentificeerd als phishing pogingen) bepaald en gerapporteerd aan de Opdrachtgever.

2. Duur

De duur van de verwerking door Opdrachtnemer is afhankelijk van de duur van de Hoofdovereenkomst. De verwerking en deze Overeenkomst inzake opdrachtspecifieke verwerking eindigen dus wanneer de Hoofdovereenkomst eindigt, voor zover er geen blijvende verplichtingen voortvloeien uit de voorwaarden van deze Overeenkomst inzake opdrachtspecifieke verwerking of deze Overeenkomst niet voortijdig wordt beëindigd. De verplichtingen uit deze overeenkomst die verder gaan dan de opdrachtspecifieke verwerking, gelden voor de betreffende periode indien een “oude” Hoofdovereenkomst wordt vervangen of gewijzigd door een “nieuwe” Hoofdovereenkomst, met vergelijkbare gegevensbeschermingsvereisten, gekoppeld aan deze Overeenkomst over de opdrachtspecifieke verwerking, en de verwerking van persoonsgegevens aldus bij afwezigheid van een Hoofdovereenkomst tijdelijk wordt voortgezet. Ononderbroken verwerking van de opdracht door de Opdrachtnemer is overeengekomen, tenzij anders geregeld door de partijen in de “vervangende” of “gewijzigde” Hoofdovereenkomst. De duur van de verwerking is dan gebaseerd op de “vervangende” of “gewijzigde” Hoofdovereenkomst.

3. Doel van de verwerking

De verwerking dient het volgende doel: de opdrachtgever moet in staat worden gesteld de door de Opdrachtnemer aangeschafte diensten inzake awareness voor gebruikers te verlenen.

4. Type en doel van het ophalen, de verwerking en het gebruik

De volgende persoonsgegevens worden verkregen en verwerkt (overeenkomstig de in de Hoofdovereenkomst vermelde dienst):

(1) Het versturen van de phishing mails

- Voor- en achternaam van de gebruikers
- Academisch niveau (optioneel)
- Werk e-mailadressen van de gebruikers
- Geslacht van de gebruikers (optioneel)
- Toegewezen gebruikersgroepen (bijv. organisatie-eenheid, locatie, rol) van de Opdrachtgever
- Eventueel verdere indelingscriteria (zie paragraaf 1.1)

- Taal van de gebruikers
- Browser/browserversie en platform van de gebruikers
- Deelname aan awareness (= geen opt-out overeenkomstig paragraaf 5)

Deze gegevens worden opgeslagen in een beveiligde database (zie bijlage III) ten behoeve van gepersonaliseerde verzending. Na voltooiing van de diensten van de Hoofdovereenkomst worden deze gegevens onherroepelijk gewist.

(2) Feedback voor gebruikers van trainingspagina's op internet

- Het bezoeken van trainingspagina's (zonder verdere datapunten zoals IP-adressen of geolocatiegegevens - deze worden niet opgehaald of via een regulier mechanisme uit de serverloggegevens verwijderd)
- Aantal bekeken tooltips/hintteksten
- Optionele feedback evaluatie of feedback vrije tekst

(3) E-learning trainingsplatform

Bij de registratie op het e-learning trainingsplatform en voor het verdere gebruik ervan:

- Voor- en achternaam van de gebruiker
- Werk e-mailadres van de gebruiker
- Taal van de gebruiker
- Geslacht van de gebruiker
- Voltooiingsstatus van de individuele e-learning trainingsmodules per gebruiker
- Resultaten van de module-quizzen per gebruiker

Ten behoeve van terugkoppeling naar de Opdrachtgever:

- Namen van de geregistreerde gebruikers
- Afrondingsstatus van alle modules (totaal)
- Gemiddeld testresultaat of procentuele juistheid van antwoorden van quizzen (totaal)
- Voltooiingsstatus van alle modules per gebruiker
- Quizwaarde of percentage nauwkeurigheid van antwoorden van quizzen per gebruiker (optioneel)

(4) Escalation Manager

Indien de Cliënt de functie Escalatiemanager heeft geboekt, worden de volgende persoonsgegevens verkregen en verwerkt. Voor escalatiedoeleinden worden deze ook naar de Klant gestuurd:

- Voor- en achternamen, werk e-mailadressen en toegewezen gebruikersgroepen van de gebruikers van Opdrachtgever
- Individuele voltooiingsstatus van alle modules
- Deadline van de campagne
- Informatie of de gebruiker een account heeft aangemaakt of niet (ja/nee)
- Informatie of de gebruiker nieuw is in de opleiding (gebruiker heeft zich in de afgelopen 90 dagen geregistreerd: ja/nee)

(5) Serverlogboeken

De volgende technische informatie wordt gedurende twaalf (12) weken tot maximaal zes (6) maanden in de serverlogboeken opgeslagen:

- IP-adressen (gepseudonimiseerd)
- User agent
- Bezochte URL
- Tijdstip

(6) Mail logboeken

De volgende technische informatie wordt gedurende twaalf (12) weken in de serverlogboeken opgeslagen:

- E-mailadres
- Afzender
- Ontvangende e-mail server
- Tijdstip

5. Categorieën van betrokkenen

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

Persoonsgegevens worden niet opgevraagd ten behoeve van de uitvoering en verwerking van de Phishingsimulatie. Geen van de gedragsgegevens (bijv. klikken op links in de gesimuleerde phishing-e-mails) wordt gekoppeld aan persoonsgegevens, maar er worden willekeurig gegenereerde codes aan toegekend en samen met deze codes opgeslagen. Deze anonimisering wordt automatisch uitgevoerd door het systeem (privacy-by-design benadering).

2. Encryptie

2.1 Gegevens in uitwisseling

Alle gegevensuitwisselingen (zowel tussen de Opdrachtgever en de Opdrachtnemer als tussen alle medewerkers van de Opdrachtnemer) worden versleuteld in overeenstemming met de aanbevelingen voor versleuteling van BSI. Met de integratie van AWS passen we de aanbevolen ELBSecurityPolicy-2016-08 van het vooraf gedefinieerde SSL-beveiligingsbeleid van AWS toe. Dit omvat TLS 1.2 met SHA 256, ECDHE sleuteluitwisseling en ECDSA voor authenticatie met AES 128 voor encryptie als minimumvereiste. Voor netwerktoegang is een VPN-verbinding nodig. Voor communicatie met service-eindpunten is een beveiligde verbinding vereist.

2.2 Gegevens in ruste

Alle persoonlijk identificeerbare Opdrachtgever- en gebruikersgegevens (bijv. e-mailadressen van gebruikers) worden versleuteld opgeslagen in beveiligde databases (autorisatiesysteem, wachtwoordbeleid met de bovengenoemde attributen, SSH-certificaat, toegang alleen mogelijk via het interne IP-gebied). Blokopslagversleuteling wordt gebruikt voor gegevens in ruste met AWS SYMMETRIC_DEFAULT_Policy. Dit betreft het symmetrische algoritme AES-256-GCM, een industriestandaard voor veilige versleuteling. Gegevens die zijn versleuteld onder AES-256-GCM zijn nu en in de toekomst beschermd omdat het wordt beschouwd als kwantumbestendig.

2.3 Gegevens in gebruik

De oplossing van de Opdrachtnemer 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 Toegangscontrole

De kantoorruimtes van de Opdrachtnemer 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 Opdrachtnemer. Bovendien is er in deze ruimten een receptie of zijn er permanent medewerkers aanwezig die voor verdere toegangscontrole zorgen. Videobewaking van alle toegangspunten is ook aanwezig.

3.2 Digitale toegangscontrole

Er zijn specifieke vereisten voor de uitgifte van wachtwoorden (willekeurig gegenereerd, minstens twaalf (12) (meestal langer wanneer we wachtwoordmanagers gebruiken) tekens lang, hoofdletters en kleine letters, cijfers en speciale tekens) voor alle systemen waarin persoonsgegevens worden verwerkt. Deze vereisten worden indien mogelijk direct geïmplementeerd in de systemen via technische maatregelen. Er wordt voor gezorgd dat alle geautoriseerde personen worden geïnformeerd dat wachtwoorden veilig moeten worden opgeslagen en niet aan andere partijen bekend mogen worden gemaakt. De aangewezen personen worden geïnstrueerd om alleen unieke wachtwoorden te gebruiken, dat wil zeggen wachtwoorden die de gebruiker niet in andere (vooral persoonlijke) systemen gebruikt. Alle systemen worden na maximaal vijf (5) minuten inactiviteit uitgeschakeld. Alle systemen beschikken over individuele antivirus- en firewallsoftware met een automatische updatefunctie.

Twee-factor authenticatie wordt gebruikt om geautoriseerde toegang te garanderen tot serversystemen die persoonsgegevens verwerken. Er wordt ook een hardware- en softwarefirewall gebruikt om het bedrijfsnetwerk van de Opdrachtnemer te beveiligen, en de Opdrachtnemer beschikt over een netwerk- en netwerkzoneconcept. Er wordt software gebruikt voor het beheer van mobiele apparaten en er wordt gebruikgemaakt van VPN-technologie voor externe toegang tot het bedrijfsnetwerk van de Opdrachtnemer.

3.3 Interne toegangscontrole

Toegang tot zowel de databasesystemen als het applicatiebeheersysteem wordt verleend op een 'need-to-know' basis, d.w.z. dat de IT-beheerder de benodigde gebruikersrechten alleen toekent aan medewerkers die belast zijn met het beheer van campagnes. Elke interne toegang tot de databasesystemen wordt gedocumenteerd en regelmatig gecontroleerd door de IT-beheerder. Deze documentatie wordt opgeslagen in een niet-wijzigbaar formaat. Dit omvat documentatie van de verleende autorisaties. De autorisaties voor productieve, test-, ontwikkelings- en administratieve systemen worden afzonderlijk toegekend.

3.4 Controle doorsturen

Het gegevensverkeer met persoonsgegevens wordt geminimaliseerd en beperkt tot de mate die nodig is om de dienst te verlenen. Aan de kant van de Opdrachtnemer hebben alleen de verantwoordelijke projectmanagers en IT-beheerders toegang tot de persoonsgegevens.

Er is een regeling voor werken op afstand. Persoonsgegevens worden verwerkt in de front-end van de SoSafe Management Software. Alle gegevensuitwisselingen (zowel tussen de Opdrachtgever en de Opdrachtnemer als tussen medewerkers van de Opdrachtnemer) naar de SoSafe Management Software zijn https-gecodeerd via AES 256bit volgens onze definities voor data in transit-encryptie. Toegang tot de databases wordt gedocumenteerd en regelmatig gecontroleerd door de IT-beheerder. Directe toegang tot de database is alleen mogelijk in het lokale bedrijfsnetwerk van de Opdrachtnemer, of via VPN als er op afstand wordt gewerkt. Alle WiFi-netwerken zijn versleuteld met WPA2. Er worden geen fysieke,

externe gegevensopslagmedia gebruikt voor bedrijfsactiviteiten.

De medewerkers van de Opdrachtnemer zijn gebonden aan het verbod op het openbaren van handels- en bedrijfsgeheimen volgens toepasselijk recht.

Er is een bring-your-own-device (BYOD) regeling van kracht. De persoonsgegevens van de Opdrachtgever waarop deze Overeenkomst betrekking heeft, w o r d t echter niet opgeslagen op de privétoestellen van de werknemers van de Opdrachtnemer. De privéapparaten (smartphones) dienen uitsluitend voor interne en externe communicatie via e-mail en samenwerkingstool (Microsoft Teams). De verwerking van de persoonsgegevens in dit verband vindt uitsluitend plaats via bedrijfsapparaten (laptops en servers) waarop de technische en organisatorische maatregelen voor gegevensbescherming zoals hier beschreven van toepassing zijn.

3.5 Verwijderen van gegevens

Er is een standaardproces voor het verwijderen van persoonsgegevens, waarvan de naleving wordt beoordeeld door zowel de IT-beheerder als de verantwoordelijke key accountmanager. Beschermingsklasse P4 volgens DIN 66399 is van toepassing op de vernietiging van fysieke gegevens.

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. Bovendien zijn alle accounts gescheiden op basis van hun werkbelasting. Opslag, computergebruik en netwerk worden onafhankelijk afgehandeld voor elke account.

4. Integriteit

Toegang tot de databases van de productieve systemen wordt vastgelegd en twaalf (12) maanden bewaard.

5. Beschikbaarheid

5.1 Beschikbaarheid garanderen

Er is een noodherstelplan beschikbaar. We beschikken over een bedrijfscontinuïteitsbeheerplan. Dit is beschreven in een bedrijfscontinuïteitsbeleid dat is gebaseerd op ISO 22301:2019 Bedrijfscontinuïteitsbeheer om de continuïteit van bedrijfsprocessen te behouden tot de operationele status op basis van

Minimaal bedrijfscontinuïteitsrendement (MBCO). Daarnaast maken we gebruik van meerdere beschikbaarheidszones binnen onze cloudarchitectuur, waardoor de uptime ook tijdens een uitval van een compleet datacenter is gegarandeerd. Van gegevens wordt dagelijks een back-up gemaakt. Alle applicaties zijn gecontaineriseerd en kunnen op verzoek opnieuw worden gebouwd en ingezet.

5.2 Doelbinding

Er zijn orderspecifieke verwerkersovereenkomsten met alle dienstverleners. Alle medewerkers van de

Opdrachtnemer 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. Duurzaamheid van systemen

De productieve systemen en servers worden voortdurend bewaakt door de serviceprovider om een constante beschikbaarheid te garanderen.

7. Herstel na incidenten

De servers en productieve systemen worden elke dag continu verzekerd via volledige back-ups. De back-ups worden versleuteld opgeslagen op afzonderlijke serversystemen van de dienstverlener. Toegang wordt verleend aan de beheerders van de Opdrachtnemer. Elke back-up wordt 30 dagen bewaard.

8. Regelmatige beoordeling van technische en organisatorische maatregelen

Er wordt een werknemer van de Opdrachtnemer aangesteld die verantwoordelijk is voor incident response management. Met het oog op de voortdurende verbetering van de informatiebeveiliging van de Opdrachtnemer worden de technische en organisatorische maatregelen ter waarborging van de gegevensbescherming en -beveiliging voortdurend door het management van de Opdrachtnemer gecontroleerd, onderzocht en verbeterd.

BIJLAGE IV – Onderaannemers

Amazon Web Services EMEA SARL (Amazon Web Services, Inc. als contractpartij van de modelcontractbepalingen van de EU)

38 avenue John F. Kennedy, L-1855, Luxemburg

Hosting van alle huidige en toekomstige componenten die benodigd zijn voor de dienstverlening, inclusief API-interface, database systeem en mailserver voor de phishing simulatie. We hebben de volgende maatregelen genomen om de gegevens te beschermen:

- Opslag en verwerking van alle gegevens in gecertificeerde datacenters in Duitsland (Frankfurt a.M.).
- Encryptie van alle klantgegevens met behulp van een door de verwerker gegenereerde hoofdsleutel, zodat noch AWS noch een andere derde partij toegang heeft tot klantgegevens, binnen of buiten de EU/EER.
- Sluiting van een gegevensverwerkingsovereenkomst alsmede de sluiting van de standaardcontractbepalingen van de EU ((EU) 2021/915, 4.6.2021, module 2 en 3), inclusief talrijke verplichtingen van AWS inzake behandeling en transparantie in geval van mogelijke verzoeken van autoriteiten.
- Transfer Impact Assessment (TIA) uitgevoerd door een externe gegevensbeschermingsdeskundige.
- Advies van een gegevensbeschermingsdeskundige over het gebruik van AWS door de verwerker, dat op verzoek kan worden verstrekt.

Hetzner Online GmbH

Industriestr. 25, 91710 Gunzenhausen

Gebruik van maildiensten voor de Phishing Simulatie van SoSafe GmbH. Indien uitdrukkelijk individueel overeengekomen met de Controller: Terbeschikkingstelling van de API-interface.

ISO27001-certificaat voor datacenters: https://www.hetzner.de/pdf/FOX_Zertifikat.pdf

salesforce.com Germany GmbH

Mail: Salesforce.com Sarl, Route de la Longeraie 9, Morges, 1110, Zwitserland, t.a.v.: Director, EMEA Sales Operations, Legal Department: Erika-Mann-Strasse 31-37, 80636, München, Duitsland.

Levering van ondersteuningssoftware (Customer Service Cloud) voor klantenservice (ondersteuningsformulier of e-mail naar support@sosafe.de). Deze provider is alleen relevant voor de Controller indien deze gebruik maakt van de klantenservice van SoSafe.
Meer informatie: https://trust.salesforce.com/

Het ISO27001-certificaat is hier toegankelijk: https://compliance.salesforce.com/en/iso-27017.

Daarnaast zijn de volgende maatregelen genomen:

- Opslag en verwerking van alle gegevens in gecertificeerde datacenters in Duitsland (Frankfurt a.M.).
- Encryptie van alle gegevens met encryptieproducten die aan de industriestandaard voldoen, zowel tijdens de overdracht als in rust.
- Sluiting van een gegevensverwerkingsovereenkomst waarin de goedgekeurde bindende bedrijfsvoorschriften (BCR) zijn opgenomen die Salesforce voor haar groepsmaatschappijen en onderaannemers heeft gesloten, alsmede de EU-standaardcontractbepalingen van 2021 met talrijke verplichtingen jegens de bevoegde toezichthoudende autoriteit en verdere vrijwillige verbintenissen.

- Transfer Impact Assessment (TIA) uitgevoerd door een externe gegevensbeschermingsdeskundige.

Microsoft Ireland Operations Ltd

One Microsoft Place, South County Business Park Leopardstown Dublin 18, D18 P521

Levering van een infrastructuur voor een e-mailserver voor communicatie met klanten in ondersteuningsgevallen via de ondersteuningssoftware (ondersteuningsformulier of e-mail naar support@sosafe.de). Deze provider is alleen relevant voor de Controller indien de Controller gebruik maakt van de klantenondersteuning van SoSafe. De volgende maatregelen zijn genomen:

- Alle gegevens worden uitsluitend binnen de Europese Unie verwerkt en opgeslagen als onderdeel van de Azure EU Cloud.
- Alle datacenters zijn ISO27001- en ISO27018-gecertificeerd: https://docs.microsoft.com/de-de/azure/security/fundamentals/infrastructure.
- Encryptie van alle gegevens met behulp van encryptieproducten die aan de industriestandaard voldoen, zowel tijdens de overdracht als in rust.
- Implementatie van de Customer Lockbox, die ervoor zorgt dat Microsoft geen toegang heeft tot de inhoud zonder de uitdrukkelijke toestemming van de verwerker.
- Sluiting van een gegevensverwerkingsovereenkomst en sluiting van de standaardcontractbepalingen van de EU ((EU) 2021/915, 4.6.2021, module 2 en 3).
- Transfer Impact Assessment (TIA) uitgevoerd door een externe gegevensbeschermingsdeskundige.

Kombo Technologies GmbH (Facultatief)

Lohmühlenstraße 65, 12435 Berlijn, Duitsland

Integratie van Client Active Directory. Deze aanbieder is alleen vereist voor zover de klant vraagt om Active Directory-integratie voor het automatisch uploaden en regelmatig bijwerken van eindgebruikersgegevens op het platform van de opdrachtnemer. De volgende maatregelen zijn genomen:

- Alle gegevens worden uitsluitend binnen de Europese Unie verwerkt en opgeslagen. Server hosting provider: Google Cloud EMEA Limited.
- Kombo Technologies GmbH is ISO27001 gecertificeerd. Toegang kan hier worden aangevraagd: https://security.kombo.dev/?itemUid=1fed9faa-4a87-427c-9a95-96b4d6bf66b7&source=click/. Meer informatie over technische en organisatorische veiligheidsmaatregelen van Kombo Technologies GmbH vindt u op security.kombo.dev.
- Codering
    - Alle klantgegevens worden gecodeerd met behulp van symmetrische AES-256 encryptie in rust, inclusief back-up kopieën.
    - Data in transit: Al het uitgaande verkeer (naar integratie-API's) gebruikt de hoogste TLS-versie die beschikbaar is door de respectievelijke API van de integratie (bijv. Google Workspace). Al het inkomende verkeer via de Kombo API is gedwongen om TLS 1.3 te gebruiken. Verbindingen van Kombo's applicatie workloads met Kombo's database gebruiken ook TLS 1.3 met een AES-256 cipher.
- Het Afsluiten van een overeenkomst voor gegevensverwerking.

SoSafe GmbH | Lichtstr. 25a | 50825 Cologne | Managing Directors: Dr. Niklas Hellemann,
Lukas Schaefer, Felix Schürholz, Felix Fichtl | HRB96220 | Amtsgericht Köln | VAT ID: DE322382415 |
Visitor address and parking: Lichtstr. 25a | 50825 Cologne | Tel: +49 (0) 221 6508 3800 |
Email: info@sosafe.de | Web: sosafe.de