Gegevensverwerkingsovereenkomst

tussen

Data Processing Agreement

Between

SoSafe GmbH

Lichtstr. 25a

en

D-50825 Keulen /Cologne

in het hiernavolgende: de
“**Opdrachtgever**” / hereafter: **Client**

in het hiernavolgende: de
“**Opdrachtnemer**” / hereafter:
Contractor

Versie / Version 2.6, bijgewerkt op / Updated on 14-11-2023

1. Inleiding, werkingssfeer, definities

(1) Deze Gegevensverwerkingsovereenkomst betreffende opdrachtspecifieke verwerking van persoonsgegevens (in het hiernavolgende: de "Overeenkomst") bepaalt de rechten en plichten van de Opdrachtgever en Opdrachtnemer met betrekking tot de verwerking van persoonsgegevens ten behoeve van een opdracht.

(2) Deze Overeenkomst is van toepassing binnen het kader van alle activiteiten waarvoor de Opdrachtnemer of door de Opdrachtnemer aangewezen onderaannemers persoonsgegevens van de Opdrachtgever verwerken.

(3) De in deze Overeenkomst gebruikte termen worden gedefinieerd overeenkomstig hun definitie in de Algemene Verordening Gegevensbescherming van de EU (in het hiernavolgende: de "AVG").

(4) De specifieke verlening van diensten (alsmede de noodzakelijke opvraging, verwerking en het gebruik van persoonsgegevens) is gebaseerd op de tussen de partijen gesloten overeenkomst betreffende de verlening van diensten inzake awareness (z.g. bewustwording) (in het hiernavolgende: de "Hoofdovereenkomst").

2. Doel en duur van de verwerking

2.1 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

1. Introduction, purview, definitions

(1) This Data Processing Agreement concerning order-specific processing of personal data (hereafter: "Contract") regulates the rights and obligations of the Client and Contractor with regard to the processing of personal information for purposes of an order.

(2) This Contract applies to all activities for which the Contractor or subcontractors appointed by the Contractor process personal information of the Client.

(3) Terms used in this Contract are defined in accordance with their definition in the EU General Data Protection Regulation (hereafter: "GDPR").

(4) The specific rendering of services (as well as the necessary retrieval, processing, and use of personal data) is based on the contract formed between the parties concerning the rendering of awareness-building services (hereafter: "Main Contract").

2. Object and duration of processing

2.1 Object

For purposes of its rendering of services, the Contractor in particular performs those activities for which personal information is processed (an exhaustive list can be found in the Main Contract):

(1) Conducting anonymous phishing simulations

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

Sending phishing mails:

- Based on the employee email addresses and employee names (hereafter: "Users") provided by the Client, the Contractor sends a defined number of email templates throughout a defined period of time.

- The email templates are personalized, i.e., they contain a personal address with the respective name of the user in order to simulate a realistic phishing attack.

- If desired by the Client, this service can be rendered in a more nuanced manner with additional categorizational criteria (e.g., organizational unit, location, status as a member of management). However, the groupings of recipients/users resulting from these categorizational criteria must always include at least five (5) persons.

- Each individual email also contains an identical link to an invisible image file (tracking pixel) that is downloaded when the email is opened.

Feedback to users when using learning pages via browser:

- The email templates each contain a unique, template-specific link (albeit identical for all the Client's users) that leads to a learning page hosted on a web server of the Contractor.

- Upon clicking on the link, the users are directed to the learning page and the respective email (without personalized address) is

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. Dit is geanonimiseerd en er worden geen persoonsgegevens geregistreerd. Als de e-mail niet van de simulatie afkomstig is, wordt hij doorgestuurd naar een door de Opdrachtgever opgegeven e-mailadres. 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

presented with an explanation of how it can be recognized as a phishing mail.

Use of the Phishing Report Button:

- An add-on for various email programs (such as Microsoft Outlook) can be optionally installed, with which users can report suspicious emails. If the respective email is from the simulation, the click is counted in the reporting rate of the evaluation, which is in turn recorded by the Contractor. This is anonymized and no personal information is recorded. If the email is not from the simulation, it is forwarded to an email addressed specified by the Client. In this case, no feedback or data flow are forwarded to the Contractor.

(2) Provision of an e-learning platform:

- Users can register for the e-learning portal on the Contractor's platform with their work email address at https://elearning.sosafe.de/registration and gain access to all e-learning modules available to them or provided by the Client. A short quiz can be taken in each module. A result is determined based on the answers (based on number of correct answers). This quiz can be repeated indefinitely.

- Alternatively, the e-learning modules can be provided to the Client as SCORM files to facilitate integration into an existing learning management system.

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 2.1 (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.

2.2 Duur

De duur van de verwerking door Opdrachtnemer is afhankelijk van de duur van de Hoofdovereenkomst. De verwerking en deze Overeenkomst inzake

(3) Provision of an evaluation (Reporting Dashboard):

- The open, reply, input, and click rates (overall and per any defined grouping by categorizational criteria, see item 2.1 (1)) can be determined based on the total number of sent emails. This information is provided to the Client via an evaluation portal – however, personalized tracking is not possible as each organizational unit must include at least five (5) persons.

- If the Contractor's platform is used for e-learning, registration rates, module progress, and results of the e-learning quizzes are recorded for the individual users and (unless otherwise agreed) reported to the Client.

- When using the Phishing Report Button, the total and categorized report rate (i.e., how many emails from the simulation have been identified by users as phishing attempts) is also determined and reported to the Client.

2.2 Duration

The duration of processing by the Contractor depends on the duration of the Main Contract. The processing and this Contract on order-specific processing thus end when the Main Contract ends, provided there are no

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.

continuous obligations stemming from the terms of this Contract on order-specific processing or this Contract is not ended prematurely. The obligations from this contract beyond the order-specific processing apply for the respective period in the event that an "old" Main Contract is superseded or amended by a "new" Main Contract, with similar data protection requirements, associated with this Contract on order-specific processing, and processing of personal information is thus transitionally continued in the absence of a Main Contract. Uninterrupted processing for the order by the Contractor is agreed, unless the Parties regulate otherwise in the "superseding" or "amended" Main Contract. The duration of the processing is then based on the "superseding" or "amended" Main Contract.

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

3.1 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.

3.2 Soort gegevens

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

3. Type and purpose of retrieval, processing, and use

3.1 Purpose of processing

The processing serves the following purpose: The Client is to be enabled to render the awareness building services purchased by the Contractor for the users.

3.2 Type of data

The following personal information is obtained and processed (according to the service specified in the Main Contract):

(1) Sending the phishing e-mails

- First and last names of users
- Academic level (optional)

- 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 2.1)
- Taal van de gebruikers
- Browser/browserversie en platform van de gebruikers
- Deelname aan awareness (= geen opt-out overeenkomstig paragraaf 3.3)

Deze gegevens worden opgeslagen in een beveiligde database (zie bijlage 1) ten behoeve van gepersonaliseerde verzending. Na voltooiing van de diensten van de Hoofdovereenkomst worden deze gegevens onherroepelijk gewist (overeenkomstig paragraaf 6 en bijlage 1).

(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

- Work e-mail addresses of users
- Sex of users (optional)
- Assigned user groups (e.g., organizational unit, location, role) of the Client
- Further categorizational criteria if required (see section 2.1)
- Language of users
- Browser/browser version and platform of users
- Participation in awareness building (= no opt-out as per section 3.3)

These data are stored in a secured database (see Annex 1) for purposes of personalized sending. After completion of the services of the Main Contract, these data are irrevocably deleted (as per section 6 and Annex 1).

(2) Feedback for users of learning pages on the Internet

- Visiting learning pages (without further data points such as IP addresses or geo-location data – these are either not retrieved or are deleted from the server log data via a regular mechanism)
- Number of tool tips/hint texts viewed
- Optional feedback evaluation or feedback free text

(3) E-learning platform

When registering on the e-learning platform and for continued use thereof:

- First and last name of the user
- Work e-mail address of the user

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:

- Language of the user
- Sex of the user
- Completion status of the individual e-learning modules per user
- Results of the module quizzes per user

For purposes of feedback to the Client:

- Names of registered users
- Completion status of all modules (aggregate)
- Average quiz result or percent accuracy of answers of quizzes (aggregate)
- Completion status of all modules per user
- Quiz value or percent accuracy of answers of quizzes per user (optional)

(4) Escalation Manager

If the Client has booked the Escalation Manager feature, the following personal information is obtained and processed. For escalation purposes it is also sent to the Client:

- First and last names, work email addresses, and assigned user groups of Client's users
- Individual completion status of all modules
- Deadline of the campaign

- 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

3.3 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

- Information whether the user has created an account or not (yes/no)
- Information if the user is new in training (user has registered in the last 90 days: yes/no)

(5) Server logs

The following technical information is stored in server logs for twelve (12) weeks to maximum six (6) months:

- IP addresses (pseudonymized)
- User agent
- URL visited
- Time

(6) Mail logs

The following technical information is stored in server logs for twelve (12) weeks:

- E-mail address
- Sender
- Receiving e-mail server
- Time

3.3 Categories of data subjects

Data subjects are, unless otherwise defined in the Main Contract, all users specified for participation by the Client. The Client is free to facilitate non-participation for individual users via an opt-out process.

individuele gebruikers mogelijk te maken via een opt-out proces.

4. Verplichtingen van de Opdrachtnemer

(1) De Opdrachtnemer verwerkt persoonsgegevens uitsluitend zoals contractueel overeengekomen of zoals opgedragen door Opdrachtgever, tenzij de Opdrachtnemer wettelijk verplicht is bepaalde verwerkingen te verrichten op grond van art. 28 para. 3 a) AVG. Indien de Opdrachtnemer aan dergelijke verplichtingen is gebonden, stelt de Opdrachtnemer de Opdrachtgever hiervan voorafgaand aan de verwerking op de hoogte, tenzij de Opdrachtnemer wettelijk verboden is dit openbaar te maken. De Opdrachtnemer dient de Opdrachtgever onmiddellijk op de hoogte te stellen indien de Opdrachtnemer meent dat een aanwijzing in strijd is met de toepasselijke wetgeving. De Opdrachtnemer kan de uitvoering van de opdracht opschorten totdat deze door de Opdrachtgever is bevestigd of gewijzigd. Bovendien gebruikt de Opdrachtnemer de voor verwerking verstrekte gegevens niet voor andere dan de contractueel overeengekomen doeleinden.

(2) De Opdrachtnemer is verplicht tot strikte geheimhouding tijdens de verwerking.

(3) De Opdrachtnemer zorgt ervoor dat het de werknemers en andere personen die verantwoordelijk zijn voor de verwerking van de gegevens verboden is de gegevens op een andere dan de opgedragen wijze te verwerken. Bovendien zorgt de Opdrachtnemer ervoor dat de personen die gemachtigd zijn de gegevens te verwerken, verplicht zijn tot geheimhouding of onderworpen zijn aan een redelijke, wettelijke geheimhoudingsplicht. De geheimhoudingsplicht blijft van kracht nadat de opdracht is voltooid.

4. Obligations of the Contractor

(1) The Contractor processes personal information solely as contractually agreed or as instructed by the Client, unless the Contractor is legally obligated to conduct certain processing pursuant to Art. 28 para. 3 a) GDPR. If the Contractor is bound to such obligations, the Contractor shall notify the Client of these in advance of the processing, unless the Contractor is legally prohibited from such disclosure. The Contractor shall immediately notify the Client if the Contractor believes that an instruction violates the applicable laws. The Contractor may suspend the implementation of the instruction until it has been confirmed or altered by the Client. Furthermore, the Contractor shall not used the data provided for processing for any other purposes other than those contractually agreed.

(2) The Contractor is obligated to strictly adhere to confidentiality during the processing.

(3) The Contractor ensures that the employees and other persons in charge of processing the data are prohibited from processing the data in any manner other than as instructed. Furthermore, the Contractor ensures that the persons authorized to process the data are bound to confidentiality or are subject to a reasonable, legal confidentiality obligation. The confidentiality/secrecy obligation remains in effect after the order has been

(4) De Opdrachtnemer zorgt ervoor dat de interne organisatie is ingericht op een wijze die geschikt is voor de specifieke vereisten inzake gegevensbescherming, en dat de door de Opdrachtnemer voor de verwerking aangestelde personen vóór het begin van de verwerking zijn geïnstrueerd over de relevante vereisten inzake gegevensbescherming en deze Overeenkomst. De desbetreffende trainings- en awareness maatregelen moeten regelmatig op passende wijze worden herzien. De Opdrachtnemer zorgt ervoor dat de personen die zijn aangesteld voor de verwerking van opdrachten voortdurend en op passende wijze worden getraind en gecontroleerd met betrekking tot de naleving van de vereisten inzake gegevensbescherming.

(5) Met betrekking tot de opgedragen verwerking dient de Opdrachtnemer de Opdrachtgever bij te staan bij het opzetten en het verdere beheer van de registratie van de verwerkingsactiviteiten en bij de beoordeling van de resultaten van de gegevensverwerking in de vereiste mate. Hierbij dient de Opdrachtnemer met name alle noodzakelijke informatie en documentatie te bewaren en deze desgevraagd zo spoedig mogelijk en binnen redelijke grenzen aan de Opdrachtgever te doen toekomen.

(6) Indien de Opdrachtgever onder toezicht is van toezichthoudende autoriteiten of andere instanties, of indien betrokkenen hun rechten doen gelden jegens de Opdrachtgever, is de Opdrachtnemer verplicht de Opdrachtgever de nodige bijstand te verlenen, mits het om de opdrachtspecifieke verwerking gaat.

(7) De Opdrachtnemer mag alleen met voorafgaande toestemming van de Opdrachtgever gegevens aan derden of betrokkenen verstrekken. De Opdrachtnemer zal alle verzoeken die rechtstreeks aan de Opdrachtnemer worden ingediend, onmiddellijk aan de

completed.

(4) The Contractor ensures that the internal organization is configured in a manner appropriate for the special requirements of data protection, and that persons appointed by the Contractor for processing have been instructed in the relevant requirements of data protection and this Contract before commencing processing. Corresponding training and sensitization measures must be regularly reviewed in a suitable manner. The Contractor ensures that the persons appointed to process orders are continuously and suitably instructed and supervised with regard to the fulfillment of the data protection requirements.

(5) In relation to the commissioned processing, the Contractor must assist the Client in the creation and continued management of the record of processing activities as well as in assessing the results of the data processing to the necessary extent, and in particular must retain all necessary information and documentation and forward these to the Client as quickly as possible, and within reasonable bounds, upon request.

(6) If the Client is subjected to monitoring by supervisory authorities or other entities, or if data subjects assert their rights to the Client, the Contractor is obligated to assist the Client to the necessary extent provided the order-specific processing is concerned.

(7) The Contractor may only render disclosure to third parties or data subjects with prior consent from the Client. The Contractor will immediately forward to the Client any

Opdrachtgever doen toekomen. De Opdrachtnemer moet direct en onmiddellijk reageren op verzoeken van toezichthoudende autoriteiten. Opdrachtnemer dient echter ook de Opdrachtgever hiervan onverwijld op de hoogte te stellen, mits de opdrachtspecifieke verwerking van persoonsgegevens van de Opdrachtgever hierdoor wordt beïnvloed.

(8) De contactgegevens van de aangewezen functionaris voor gegevensbescherming staan altijd opgeslagen in het privacybeleid op de website van de Opdrachtnemer op https://sosafe-awareness.com/privacy-policy.

(9) De opdrachtspecifieke verwerking vindt uitsluitend binnen de EU plaats. Verplaatsing naar een derde land is alleen mogelijk met toestemming van de Opdrachtgever en in overeenstemming met de voorwaarden in hoofdstuk V van de AVG en met inachtneming van de voorwaarden van deze Overeenkomst.

5. Technische en organisatorische maatregelen

(1) De in bijlage 1 genoemde maatregelen voor gegevensbeveiliging zijn bindend. Deze bepalen het door de Opdrachtnemer aanvaarde minimum. De beschrijving van de maatregelen moet zodanig gedetailleerd zijn dat een goed geïnformeerde derde partij op basis van enkel de beschrijving met zekerheid kan vaststellen wat het aanvaarde minimum zou moeten zijn.

(2) De gegevensbeveiligingsmaatregelen kunnen worden aangepast aan de verdere technische en organisatorische ontwikkeling, waarbij ook software-updates van de fabrikant worden meegenomen, mits ten minste aan het hier overeengekomen beveiligingsniveau wordt voldaan. De Opdrachtnemer moet onmiddellijk alle wijzigingen doorvoeren

requests submitted directly to the Contractor. The Contractor must directly and immediately respond to any requests from supervisory authorities. However, the Contractor must also immediately notify the Client of this provided the order-specific processing of personal information of the Client is hereby affected.

(8) The contact information of the appointed data protection officer is always stored in the privacy policy on the website of the Contractor at https://sosafe-awareness.com/privacy-policy.

(9) The order-specific processing occurs solely within the EU. Any relocation to a third country is only possible with consent from the Client and in accordance with the conditions in Chapter V of the GDPR as well as with adherence to the terms of this Contract.

5. Technical and organizational measures

(1) The data security measures specified in Annex 1 are binding. They define the minimum accepted by the Contractor. The description of the measures must be so detailed that a knowledgeable third party should be able to determine with certainty what the accepted minimum should be based on the description alone.

(2) The data security measures can be adjusted according to the further technical and organizational development, whereby software updates by the manufacturer are also included, as long as the level of security agreed herein is at least fulfilled. The Contractor must immediately implement any changes required to ensure information security. Changes must immediately be reported to the Client.

die nodig zijn om de informatiebeveiliging te waarborgen. Wijzigingen moeten onmiddellijk aan de Opdrachtgever worden gemeld.

(3) Indien de desbetreffende beveiligingsmaatregelen niet (meer) aan de behoeften van de Opdrachtgever voldoen, stelt de Opdrachtnemer de Opdrachtgever daarvan onverwijld op de hoogte.

(4) Kopieën of duplicaten mogen niet worden gemaakt zonder medeweten van de Opdrachtgever. Technisch noodzakelijke, tijdelijke duplicaties zijn uitgesloten, mits deze geen afbreuk doen aan het hier overeengekomen niveau van gegevensbescherming.

(5) De Opdrachtnemer controleert regelmatig zijn verplichtingen, met name de volledige uitvoering van de overeengekomen technische en organisatorische maatregelen en de doeltreffendheid daarvan. De verificatie moet op verzoek aan de Opdrachtgever worden voorgelegd. Deze verificatie kan plaatsvinden via overeengekomen gedragscodes of een overeengekomen certificeringsproces.

6. Verordening inzake de correctie, verwijdering en afscherming van gegevens

(1) De Opdrachtnemer zal de verwerkte persoonsgegevens voor opdrachtspecifieke doeleinden alleen corrigeren, verwijderen of afschermen in overeenstemming met de contractuele overeenkomst of op instructie van de Opdrachtgever, mits dit in de parameters van de instructies is opgenomen. De beheerinterface maakt het voor de klant mogelijk om de gegevens van de eindgebruikers te wijzigen of te verwijderen. De Opdrachtnemer is slechts in tweede instantie verplicht bijstand te verlenen met betrekking tot de correctie,

(3) If the security measures concerned do not or no longer meet the needs of the Client, the Contractor shall immediately notify the Client of this.

(4) Copies or duplicates are not created without the Client's knowledge. This excludes technically required, temporary duplications, provided this does not impair the level of data protection agreed herein.

(5) The Contractor regularly renders verification of its obligations, in particular the full implementation of the agreed technical and organizational measures as well as the efficacy thereof. The verification must be presented to the Client on request. This verification can be rendered via agreed codes of conduct or an agreed certification process.

6. Regulation on the correction, deletion, and blocking of data

(1) The Contractor will only correct, delete, or block personal data processed for order-specific purposes in accordance with the contractual agreement or as instructed by the Client, provided such is included in the parameters of the instructions. The admin interface makes it possible for the customer to modify or delete the end users' data. The Contractor is only secondarily obligated to provide assistance with regard to the correction, deletion, or blocking via the admin interface.

verwijdering of afscherming via de beheerinterface.

(2) De Opdrachtnemer zal zich altijd houden aan de door de Opdrachtgever verstrekte instructies, zelfs na beëindiging van deze Overeenkomst.

(3) Bij beëindiging van deze contractuele relatie, of indien de Opdrachtgever hiernaar vraagt, moet de Opdrachtnemer de gegevens die onderworpen zijn aan opdrachtspecifieke verwerking teruggeven aan de Opdrachtgever of vernietigen op een wijze die in overeenstemming is met de bescherming van persoonsgegevens. De Opdrachtgever kiest welke optie wordt gekozen. Alle kopieën van de gegevens moeten ook worden vernietigd. Deze vernietiging moet zodanig worden uitgevoerd dat het zelfs niet mogelijk is om met een redelijke inspanning restinformatie te reproduceren.

(4) De Opdrachtnemer is verplicht ook onderaannemers aan te zetten tot onmiddellijke teruggave of verwijdering.

(5) De Opdrachtnemer moet de correcte vernietiging verifiëren. Wanneer alle gegevens van de Opdrachtgever zijn verwijderd (verwijdering van de opdrachtgever uit de SoSafe Management Software), wordt een verwijderingsrapport gegenereerd dat het tijdstip en de omvang van de verwijdering documenteert. Dit verwijderingsrapport moet op verzoek onmiddellijk aan de Opdrachtgever worden voorgelegd.

(6) De Opdrachtnemer heeft geen eigendomsvoorbehoud op materialen en werkresultaten.

(7) Documentatie die dient om de juiste gegevensverwerking te verifiëren, moet ook door de Opdrachtnemer worden bewaard overeenkomstig de respectieve bewaartermijnen, ook na afloop van de

(2) The Contractor will always abide by the instructions issued by the Client, even after this Contract has ended.

(3) Upon the end of this Contract relationship, or at any time at the Client's request, the Contractor must either destroy the data subjected to order-specific processing in a manner compliant with data protection, or return these to the Client. The Client selects which option is to be chosen. All copies of the data must also be destroyed. This destruction must be conducted such that it is not possible to reproduce even residual information with reasonable effort.

(4) The Contractor is obligated to induce immediate return or deletion by subcontractors as well.

(5) The Contractor must render verification of proper destruction. When all the Client's data are deleted (client deletion from the SoSafe Management Software), a deletion report is generated that documents the time and scope of the deletion. This deletion report shall immediately be presented to the Client upon request.

(6) The Contractor has no right of retention to materials and work results.

(7) Documentation that serves to verify proper data processing must also be retained by the Contractor in accordance with the respective retention periods, including beyond the end of the Contract period. The Contractor may provide this

termijn van de Overeenkomst. De Opdrachtnemer kan deze documentatie aan het einde van de termijn van de Overeenkomst aan de Opdrachtgever verstrekken.

documentation to the Client upon the end of the Contract period.

7. Uitbesteding

(1) Het inschakelen van onderaannemers door de Opdrachtnemer is alleen toegestaan indien de Opdrachtgever hiervoor toestemming heeft verleend. Deze toestemming wordt geacht te zijn verleend voor de in bijlage 2 vermelde onderaannemers. De aanstelling of wijziging van een andere onderaannemer door de Opdrachtnemer moet vóór de aanstelling schriftelijk of in tekstvorm aan de Opdrachtgever worden gemeld. De Opdrachtgever beschikt vervolgens over 14 kalenderdagen, die ingaan vanaf de indiening van de te onderzoeken documenten, om in geval van een dwingende oorzaak tegen deze benoeming in beroep te gaan. Een dwingende oorzaak is met name aanwezig wanneer er objectieve aanwijzingen zijn dat de onderaannemer niet in staat is aan gegevensbescherming en contractuele vereisten te voldoen. In geval van een gegrond beroep kan de Opdrachtnemer besluiten de onderaannemer niet in te zetten. Indien de Opdrachtnemer ondanks het gerechtvaardigde beroep van de Opdrachtgever besluit de onderaannemer in te zetten, heeft de Opdrachtgever na kennisneming van de omstandigheden (tewerkstelling van de onderaannemer ondanks het beroep) zeven (7) kalenderdagen de tijd om een bijzonder recht tot opzegging van deze Overeenkomst zonder opzeggingstermijn uit te oefenen. Nadat 14 dagen zijn verstreken zonder beroep, wordt de toestemming geacht te zijn verleend.

(2) De inschakeling van onderaannemers als bijkomende (onder)aannemers om de diensten van de Opdrachtnemer te vervullen is alleen mogelijk als de

7. Subcontracting

(1) The employment of subcontractors by the Contractor is only permitted with consent from the Client. This consent is considered granted for the subcontractors specified in Annex 2. The appointment or change of another subcontractor by the Contractor must be reported to the Client in writing or text form before the appointment. The Client then receives 14 calendar days, beginning with the submission of the documents to be examined, to appeal against this appointment in the event of compelling cause. Compelling cause in particular is present when there are objective indications that the subcontractor is not capable of fulfilling the data protection and contractual requirements. In the event of a justified appeal, the Contractor may decide not to employ the subcontractor. If the Contractor decides to employ the subcontractor despite the justified appeal by the Client, the Client has seven (7) calendar days after becoming aware of the circumstances (employment of the subcontractor in spite of appeal) to exercise a special right of cancellation of this agreement without notice. After 14 days have passed without appeal, the consent is considered granted.

(2) The employment of subcontractors as additional (sub-)contractors to fulfil the Contractor's services is only possible if the subcontractor has at least been bound to data protection obligations that are

onderaannemer in ieder geval gebonden is aan gegevensbeschermingsverplichtingen die vergelijkbaar zijn met die welke in deze Overeenkomst zijn vermeld, en dat ten minste aan het niveau van gegevensbescherming wordt voldaan. Op verzoek kan de Opdrachtgever inzicht verkrijgen in de relevante onderdelen van de Overeenkomst tussen de Opdrachtnemer en de onderaannemer.

(3) De rechten van de Opdrachtgever ten opzichte van de onderaannemer moeten daadwerkelijk kunnen worden uitgeoefend. In het bijzonder moet de Opdrachtgever te allen tijde gemachtigd zijn om toezicht uit te oefenen op onderaannemers, of dit toezicht door derden te laten uitvoeren, binnen het toepassingsgebied dat hierin gespecificeerd is.

(4) De verantwoordelijke partijen van de Opdrachtnemer en van de onderaannemer moeten duidelijk van elkaar gescheiden zijn.

(5) De Opdrachtnemer selecteert de onderaannemer zorgvuldig en let daarbij in het bijzonder op de geschiktheid van de technische en organisatorische maatregelen van de onderaannemer.

(6) De inschakeling van onderaannemers die niet uitsluitend opdrachtspecifieke gegevensverwerking binnen de EU of de EER uitvoeren, is alleen mogelijk in overeenstemming met de in paragraaf 4 (9) van deze Overeenkomst genoemde voorwaarden. Het is met name alleen toegestaan indien en zolang de onderaannemer passende garanties inzake gegevensbescherming biedt. De Opdrachtnemer stelt de Opdrachtgever op de hoogte van de specifieke garanties inzake gegevensbescherming die de onderaannemer biedt, en van de wijze waarop dit kan worden geverifieerd.

comparable to those specified in this Contract, and that the level of data protection is at least met. Upon request the Client receives insight into the relevant Contract components between the Contractor and subcontractor.

(3) It must be possible for the rights of the Client to be effectively exercised relative to the subcontractor. In particular, the Client must be authorized at any time to conduct monitoring of subcontractors, or allow such monitoring by third parties, in the scope specified herein.

(4) The Contractor's and subcontractor's responsible parties must be clearly demarcated from each other.

(5) The Contractor carefully selects the subcontractor with special consideration of the suitability of the technical and organizational measures taken by the subcontractor.

(6) The employment of subcontractors who do not exclusively conduct order-specific data processing within the EU or the EEA is only possible in accordance with the conditions listed in section 4 (9) of this Contract. In particular, it is only permissible if and as long as the subcontractor makes appropriate data protection guarantees. The Contractor shall notify the Client of the specific data protection guarantees offered by the subcontractor, and how to obtain verification of this.

(7) The Contractor must regularly and reasonably assess adherence to the

(7) De Opdrachtnemer moet de naleving van de verplichtingen van de onderaannemer regelmatig en op redelijke wijze beoordelen. De beoordeling en de resultaten daarvan moeten grondig worden gedocumenteerd, zodat deze voor een deskundige derde partij begrijpelijk zijn. De documentatie moet op verzoek aan de Opdrachtgever worden voorgelegd.

(8) Indien de onderaannemer zijn verplichtingen inzake gegevensbescherming niet nakomt, is de Opdrachtnemer hiervoor aansprakelijk tegenover de Opdrachtgever.

(9) Bij de afsluiting van deze Overeenkomst worden de in bijlage 2 vermelde onderaannemers met hun naam, adres en diensten ingezet om persoonsgegevens te verwerken in het betreffende toepassingsgebied dat daarin wordt vermeld, en worden zij door de Opdrachtgever goedgekeurd. De overige verplichtingen van de Opdrachtnemer jegens de onderaannemers die hierin zijn vermeld, blijven onverlet.

(10) Uitbestede diensten conform deze Overeenkomst omvatten alleen de diensten die rechtstreeks verband houden met het verlenen van de hoofddienst. Hulpdiensten, zoals telecommunicatiediensten of gebruikersdiensten (tenzij verplicht volgens de Hoofdovereenkomst) zijn niet inbegrepen. De verplichting van de Opdrachtnemer om in deze gevallen de gegevensbescherming en -beveiliging in acht te nemen, blijft onverminderd van kracht.

8. Rechten en verplichtingen van de Opdrachtgever

(1) De Opdrachtgever is als enige verantwoordelijk voor de naleving van de wettelijke bepalingen van de wetgeving inzake gegevensbescherming, met name de rechtmatigheid van de verstrekking van

subcontractor's obligations. The assessment and results thereof must be thoroughly documented such that they are comprehensible to a knowledgeable third party. The documentation must be submitted to the Client on request.

(8) If the subcontractor fails to meet their data protection obligations, the Contractor is liable for this to the Client.

(9) Upon finalization of this Contract, the subcontractors specified in Annex 2 with their name, address, and services are employed to process personal information in the respective scope mentioned therein, and are accepted by the Client. The other obligations of the Contractor to the subcontractors specified herein remain unaffected.

(10) Subcontracting services in accordance with this Contract only include those services directly pertaining to the rendering of the main service. Auxiliary services, such as telecommunication services or user service (unless owed as per the Main Contract) are not included. The Contractor's obligation to ensure adherence to data protection and data security in these instances remains unaffected.

8. Rights and obligations of the Client

(1) The Client is solely responsible for adhering to the legal provisions of the data protection laws, in particular the legality of data disclosure to the Contractor and of data processing and preserving data

gegevens aan de Opdrachtnemer en van de gegevensverwerking en het behoud van de rechten van de betrokkenen, voor zover het de verantwoordelijke partij betreft.

subject rights, provided these concern the responsible party.

(2) De Opdrachtgever verstrekt alle opdrachten, deelopdrachten of instructies, alsmede wijzigingen, aanvullingen of vervangingen daarvan in schriftelijke of elektronische vorm (tekstvorm). In zeer dringende gevallen kunnen mondelinge instructies worden gegeven. Mondelinge instructies moeten door de Opdrachtgever onmiddellijk schriftelijk of in tekstvorm worden bevestigd.

(2) The Client issues all orders, sub-orders, or instructions, as well as changes, supplements, or replacements thereof in written or an electronic format (text form). In cases of particular urgency, verbal instructions can be issued. Verbal instructions must immediately be confirmed in writing or text form by the Client.

(3) De Opdrachtgever stelt de Opdrachtnemer onmiddellijk op de hoogte indien bij de beoordeling van de verwerkingsresultaten of met betrekking tot de gegevensbeschermingsvoorschriften fouten of discrepanties worden vastgesteld.

(3) The Client shall immediately notify the Contractor if it discovers errors or discrepancies during the assessment of the processing results or with regard to the data protection requirements.

(4) De Opdrachtgever is bevoegd op redelijke wijze toezicht te houden (of opdracht te geven om op redelijke wijze toezicht te houden) op de naleving van de voorschriften en vereisten inzake gegevensbescherming van de contractuele overeenkomsten met de Opdrachtnemer, met name door het inwinnen van informatie en het bekijken van de opgeslagen gegevens en de gegevensverwerkingsprogramma's, alsmede door andere inspecties ter plaatse. De Opdrachtnemer moet de toezichthoudende personen indien nodig toegang en inzicht verschaffen. De Opdrachtnemer is verplicht de nodige informatie te verstrekken, processen aan te tonen en de voor het toezicht vereiste verificaties te verrichten. Indien een derde partij de inspectie uitvoert, dient deze derde partij gebonden te zijn aan gegevens- en geheimhoudingsbescherming zoals

(4) The Client is authorized to reasonably monitor (or commission the reasonable monitoring of) adherence to the data protection regulations and requirements of the contractual agreements with the Contractor, in particular by obtaining information and viewing the stored data and data processing programs, as well as other on-site inspections. The Contractor must grant access and insight to the monitoring persons as necessary. The Contractor is obligated to issue the necessary information, demonstrate processes, and render verification required for monitoring. If a third party is conducting the inspection, this third party must be bound to data and secret protection as described in section 7 of the SoSafe Terms and Conditions.

beschreven in paragraaf 7 van de SoSafe Voorwaarden.

(5) Inspecties in de gebouwen van de Opdrachtnemer mogen niet leiden tot vermijdbare belemmeringen van diens bedrijfsvoering. Tenzij er dringende redenen zijn die door de Opdrachtgever moeten worden gedocumenteerd, mogen inspecties alleen worden uitgevoerd na een redelijke aankondigingstermijn en tijdens de werkuren van de Opdrachtnemer, en niet vaker dan om de twaalf (12) maanden. Indien de Opdrachtnemer verificatie verricht van de juiste implementatie van de overeengekomen verplichtingen op het gebied van gegevensbescherming, zal de inspectie beperkt blijven tot steekproeven. Indien de door de Opdrachtgever aangewezen inspecteur in concurrentie is met de Opdrachtnemer, heeft de Opdrachtnemer het recht hiertegen in beroep te gaan.

(5) Inspections on the Contractor's premises must not result in any avoidable impairments of its business operations. Unless otherwise induced by urgent reasons that the Client must document, inspections must only be conducted following a reasonable notice period and during the Contractor's hours of operation, and not more often than every twelve (12) months. If the Contractor renders verification of the proper implementation of the agreed data protection obligations, inspection shall be limited to random sampling. If the inspector appointed by the Client is in competition with the Contractor, the Contractor has the right to appeal this.

9. Kennisgevingsverplichtingen

(1) De Opdrachtnemer dient de Opdrachtgever onmiddellijk op de hoogte te stellen in geval van inbreuken op de beveiliging van persoonsgegevens. Ook gerechtvaardigde gevallen van verdenking moeten worden gemeld. Deze melding dient uiterlijk 24 uur nadat Opdrachtnemer kennis heeft genomen van het betreffende voorval te geschieden aan een door Opdrachtgever aangewezen partij. Het moet ten minste de volgende informatie bevatten:

a. een beschrijving van het soort inbreuk op de beveiliging van persoonsgegevens, zo mogelijk met vermelding van de categorieën en een geschat aantal betrokken persoonsgegevens verzamelingen;

b. de naam en contactgegevens van de functionaris voor

9. Notification obligations

(1) The Contractor shall immediately notify the Client of violations of the security of personal information. Justified instances of suspicion must also be reported. This reporting must be rendered no later than 24 hours after the Contractor has become aware of the relevant incident, and directed to a party specified by the Client. It must contain at least the following information:

a. a description of the type of violation of the security of personal information, if possible with specification of the categories and approximate number of affected personal data sets;

b. the name and contact information of the data protection officer or

gegevensbescherming of een andere contactpersoon voor nadere informatie;

c. een beschrijving van de waarschijnlijke gevolgen van de inbreuk op de beveiliging van persoonsgegevens;

d. een beschrijving van de door de Opdrachtnemer genomen of voorgestelde maatregelen om de schending van de beveiliging van persoonsgegevens te verhelpen en, in voorkomend geval, maatregelen om eventuele negatieve gevolgen daarvan op te vangen.

(2) Belangrijke verstoringen van de dienstverlening, en schendingen door de Opdrachtnemer of zijn werknemers jegens gegevensbeschermingsvoorschriften of de bepalingen in deze Overeenkomst, moeten ook onmiddellijk worden gemeld.

(3) De Opdrachtnemer dient de Opdrachtgever onmiddellijk op de hoogte te stellen van inspecties of maatregelen van toezichthoudende autoriteiten of andere derde partijen, voor zover deze betrekking hebben op de opdrachtspecifieke verwerking.

(4) De Opdrachtnemer dient voor zover noodzakelijk de Opdrachtgever te ondersteunen bij zijn verplichtingen overeenkomstig Art. 32-36 AVG.

10. Instructies

(1) De Opdrachtgever behoudt zich een uitgebreid instructierecht voor in het kader van de opdrachtgebaseerde verwerking.

other contact for further information;

c. a description of the likely consequences of the violation of the security of personal information;

d. a description of the measures taken or suggested by the Contractor to remedy the violation of the security of personal information and, if applicable, measures for alleviating any potentially negative consequences thereof.

(2) Significant disruptions to the rendering of services, and violations by the Contractor or its employees against data protection regulations or the determinations made in this Contract, must also immediately be reported.

(3) The Contractor shall immediately notify the Client of inspections or measures by supervisory authorities or other third parties, provided these pertain to the order-specific processing.

(4) The Contractor ensures that it shall support the Client to the necessary extent with its obligations pursuant to Art. 32-36 GDPR.

10. Instructions

(1) The Client reserves a comprehensive right of instruction for purposes of order-based processing.

(2) The Client and Contractor appoint the sole persons authorized to issue and receive

(2) De Opdrachtgever en de Opdrachtnemer wijzen in bijlage 3 de personen aan die als enige bevoegd zijn tot het geven en ontvangen van instructies.

(3) In geval van wijziging of langdurige verhindering van deze aangewezen personen moet de andere partij onmiddellijk op de hoogte worden gesteld indien er opvolgers of vertegenwoordigers zijn.

(4) De Opdrachtnemer dient de Opdrachtgever op de hoogte te stellen indien hij meent dat een door Opdrachtgever gegeven instructie in strijd is met de wettelijke voorschriften. De Opdrachtnemer is bevoegd de uitvoering van de desbetreffende instructie op te schorten totdat deze is bevestigd of gewijzigd door de verantwoordelijke partij die de Opdrachtgever vertegenwoordigt.

(5) De Opdrachtnemer moet de opgegeven instructies en de uitvoering daarvan documenteren.

instructions in Annex 3.

(3) In the event of a change in or long-term inability of these appointed persons, the other party must immediately be notified of successors or representatives.

(4) The Contractor must notify the Client if it believes that an instruction issued by the Client violates legal regulations. The Contractor is authorized to suspend the rendering of the respective instruction until it has been confirmed or altered by the responsible party representing the Client.

(5) The Contractor must document instructions issued to it and the rendering thereof.

11. Verzoeken van betrokkenen

Indien een betrokkene contact opneemt met de Opdrachtnemer met een claim betreffende de rechten van de betrokkene op grond van art. 12 AVG, zal de Opdrachtnemer de betrokkene doorverwijzen naar de Opdrachtgever indien toewijzing aan de Opdrachtgever mogelijk is volgens de verklaringen van de betrokkene. De Opdrachtnemer geeft het verzoek van de betrokkene onmiddellijk door aan de Opdrachtgever. De Opdrachtnemer staat de Opdrachtgever bij zoals opgedragen en overeengekomen.

11. Data subject rights

If a data subject contacts the Contractor with a claim concerning data subject rights as per Art. 12 GDPR, the Contractor will refer the data subject to the Client if assignment to the Client is possible according to the statements made by the data subject. The Contractor immediately forwards the data subject's request to the Client. The Contractor assists the Client as instructed and as agreed.

12. Vergoeding

De vergoeding van de Opdrachtnemer is definitief vastgesteld in de Hoofdovereenkomst. Er is geen afzonderlijke

12. Compensation

The Contractor's compensation is definitively regulated in the Main Contract. There is no separate compensation or reimbursement of costs for purposes of this Contract.

vergoeding of terugbetaling van kosten in het kader van deze Overeenkomst.

13. Aansprakelijkheid

De bepalingen van de AVG, in het bijzonder art. 82 AVG, en Art. 28 par. 4 zin 2 AVG in geval van gebruik van een onderaannemer, zijn van toepassing.

14. Bijzonder recht van opzegging

(1) De Opdrachtgever kan deze Overeenkomst te allen tijde opzeggen zonder inachtneming van een termijn ("opzegging zonder kennisgeving") in geval van een ernstige schending van de voorschriften inzake gegevensbescherming door de Opdrachtnemer, of indien de Opdrachtnemer in strijd met de Overeenkomst de controlerechten van de Opdrachtgever ontkent.

(2) Er is met name sprake van een ernstige schending indien de Opdrachtnemer de in deze Overeenkomst omschreven verplichtingen, met name de overeengekomen technische en organisatorische maatregelen, niet of onvoldoende nakomt.

(3) Bij ernstige schending verleent de Opdrachtgever de Opdrachtnemer een voldoende lange hersteltermijn. Indien niet tijdig wordt gereageerd, is de Opdrachtgever gerechtigd deze Overeenkomst op te zeggen zonder voorafgaande kennisgeving zoals beschreven in deze paragraaf.

15. Diverse

(1) Beide partijen zijn verplicht tot geheimhouding van alle kennis van bedrijfsgeheimen en gegevensbeschermingsmaatregelen van de respectieve andere partij die zij in het kader van de contractuele relatie hebben verkregen, ook na afloop van de termijn van de Overeenkomst. Indien er enige

13. Liability

The terms of the GDPR, in particular Art. 82 GDPR, and Art. 28 para. 4 sentence 2 GDPR in the event of use of a subcontractor, apply.

14. Special right of cancelation

(1) The Client can cancel this Contract at any time without adherence to a term ("cancelation without notice") in the event of a grave violation against data protection regulations by the Contractor, or if the Contractor denies the Client's monitoring rights in violation of the Contract.

(2) In particular, a grave violation has occurred if the Contractor does not fulfil or has not sufficiently fulfilled the obligations defined in this Contract, in particular the agreed technical and organizational measures.

(3) In the event of grave violations, the Client grants the Contractor a sufficient remedy period. If remedy is not rendered in a timely fashion, the Client is authorized to cancel this Contract without notice as described in this section.

15. Miscellaneous

(1) Both parties are obligated to treat with confidentiality all knowledge of trade secrets and data protection measures of the respective other party obtained due to the contract relationship, including beyond the end of the Contract period. If there is any doubt as to whether a piece of information is subject to the confidentiality obligation, it must be treated as confidential until written approval by the other party has been rendered.

twijfel bestaat over de vraag of een gegeven onder de geheimhoudingsplicht valt, moet het als vertrouwelijk worden behandeld totdat de andere partij er schriftelijk mee heeft ingestemd.

(2) Indien eigendom van de Opdrachtgever dat zich in handen van de Opdrachtnemer bevindt door maatregelen van derden (bijv. door verpanding of confiscatie), insolventie- of schikkingsprocedures of andere gebeurtenissen in gevaar komt, dient de Opdrachtnemer de Opdrachtgever hiervan onverwijld op de hoogte te stellen. De Opdrachtnemer dient alle betrokken verantwoordelijke partijen onmiddellijk op de hoogte te stellen dat de soevereiniteit en de eigendom van de gegevens uitsluitend berusten bij de Opdrachtgever als “verantwoordelijke partij” overeenkomstig de AVG.

(3) Voor wijzigingen van deze Overeenkomst, bijkomende overeenkomsten en verklaringen in deze Overeenkomst is een schriftelijke vorm op grond van § 126 BGB (Duits Burgerlijk Wetboek) vereist, zodat ook e-mails aan deze schriftelijke vormvereiste voldoen.

(4) Een beroep op het recht van bewaring op grond van § 273 BGB (Duits Burgerlijk Wetboek) is uitgesloten met betrekking tot de gegevens die worden onderworpen aan opdrachtspecifieke verwerking en de respectieve gegevensdragers.

(5) Indien afzonderlijke onderdelen van deze Overeenkomst ongeldig zijn, wordt de geldigheid van de rest van de Overeenkomst niet beïnvloed.

(6) De wetten van de Bondsrepubliek Duitsland zijn van toepassing.

(7) Deze Gegevensverwerkingsovereenkomst voorwaarden zijn opgesteld in het Engels en in het Nederlands. In geval van tegenstrijdigheden tussen deze twee versies van de

(2) Should the any of the Client's property in the Contractor's possession be endangered due to third-party measures (e.g., via pledge or confiscation), insolvency or conciliation proceedings, or other events, the Contractor must immediately notify the Client. The Contractor will immediately notify all concerned responsible parties that the sovereignty and ownership of the data lie solely with the Client as the "responsible party" in accordance with the GDPR.

(3) Written form pursuant to § 126 BGB is required for changes to this Contract, collateral agreements, and declarations made in this Contract, to which end e-mails also fulfill this written form requirement.

(4) Appeal of the right of retention pursuant to § 273 BGB is ruled out with regard to the data subjected to order-specific processing and respective data storage media.

(5) Should individual components of this agreement be invalid, the validity of the reminder of the agreement is not affected.

(6) The laws of the Federal Republic of Germany apply.

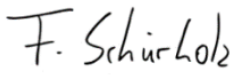
(7) This Data Processing Agreement is hereby drawn up in English and in Dutch version. In case of contradiction(s) between these two versions of this Data Processing Agreement, the English version shall prevail.

Gegevensverwerkingsovereenkomst voorwaarden heeft de Engelse versie voorrang.

Handtekeningen / Signatures

Plaats, datum /Place, date:

Keulen / Cologne, op /on



Client/ Opdrachtgever

Contractor/ Opdrachtnemer

Annex 1 - Technical and organizational measures

The technical and organizational measures for ensuring data protection and data security, which the Contractor must at least establish and continuously uphold, are defined below. The goal in particular is the guarantee of confidentiality, integrity, and availability of the information subject to order-specific processing.

1. Anonymization

Personal information is not retrieved for purposes of the execution and processing of the Phishing Simulation. None of the behavioral data (e.g., clicks on links in the simulated phishing e-mails) are not associated with personal information, but rather assigned randomly generated codes and stored in conjunction with these codes. This anonymization is automatically performed by the system (privacy-by-design approach).

2. Encryption

2.1 Data in transfer

All data transfers (both between the Client and the Contractor as well as between all employees of the Contractor) are encrypted in accordance with the recommendations for encryption from BSI. With the integration of AWS, we apply the recommended ELBSecurityPolicy-2016-08 from AWS predefined SSL security policies, This includes TLS 1.2 with SHA 256, ECDHE key exchange and ECDSA for authentication with AES 128 for encryption as a minimum requirement. Network

access requires a VPN connection. Communication with service endpoints require a secure connection.

2.2 Data at rest

All personally identifiable Client and user data (e.g., user e-mail addresses) are encrypted when stored in protected databases (authorization system, password policy with the aforementioned attributes, SSH certificate, access only possible via the internal IP area). Block storag-e encryption is used for data at rest using AWS SYMMETRIC_DEFAULT_Policy. This represents AES-256-GCM symmetric algorithm which is an industry standard for secure encryption. Data encrypted under AES-256-GCM is protected now and in the future as it is considered quantum resistant.

2.3 Data in use

The Contractor's solution concerns a pure cloud application with which the front end on the end user's computer is operated. This offers no possibility for encryption.

3. Confidentiality

3.1 Access control

The Contractor's office spaces are only accessible with the respective keys or transponders with matching security locks. The issuance of keys and transponders is documented and countersigned by the Contractor's management. Furthermore, there is in these spaces a reception or permanently present employees who ensure further access control. Video monitoring of all access points is also present.

3.2 Digital access control

There are specific requirements for the issuance of passwords (randomly generated, at least twelve (12) (usually longer where we use password managers)_ characters long, upper and lower case, numbers, and special characters) for all systems in which personal information is processed. These requirements are directly implemented in the systems via technical measures if possible. It is ensured that all authorized persons are informed that passwords must be stored securely and must not be disclosed to other parties. The appointed persons are instructed to only use unique passwords, i.e., passwords that the user does not use in any other (especially personal) systems. All clients are timed out after no more than five (5) minutes of inactivity. All clients possess an individual antivirus and firewall software with an automatic update function.
Two-factor authentication is used to ensure authorized access to server systems that process personal information. A hardware and software firewall is also used to secure the Contractor's company network, and the Contractor possesses a network and network zone concept. Mobile device management software is used, and VPN technology is employed for external access to the Contractor's company network.

3.3 Internal access control

Access to both the database systems and the application management system is granted on a need-to-know basis, i.e., the IT administrator issues the user rights as necessary only to those employees entrusted with the administration of campaigns. Every instance of internal access to the database systems is documented and regularly inspected by the IT

administrator. This documentation is saved in a non-editable format. This comprises documentation of the granted authorizations. The authorizations for productive, testing, development, and administrative systems are granted separately.

3.4 Forwarding control

Data traffic with personal information is minimized and limited to the extent required to render the service. On the Contractor side, only the responsible project managers and IT administrators have access to the personal information.

A remote work regulation is in place. Personal information is processed in the front end of the SoSafe Management Software. All data transfers (both between the Client and the Contractor as well as between employees of the Contractor) to the SoSafe Management Software are https-encrypted via AES 256bit following our data in transit encryption definitions. Access to the databases is documented and regularly inspected by the IT administrator. Direct database access is only possible in the local company network of the Contractor, or via VPN when working remotely. All WiFi networks are encrypted with WPA2. No physical, external data storage media are used for business operations.

The Contractor's employees are bound to the prohibition on the betrayal of trade and business secrets as per the Trade Secret Act (*Geschäftsgeheimnisgesetz*) as well as the purpose limitation and confidentiality obligation as per § 78 para. 1 SGB X.

A bring-your-own-device (BYOD) regulation is in place. However, the Client's personal information that this Contract concerns is not stored on the Contractor's employees' private

devices. The private devices (smartphones) solely serve the purpose of internal and external communication via e-mail and collaboration tool (Microsoft Teams). The processing of the personal information concerned here is solely conducted via company devices (laptops and servers) to which the technical and organizational measures for data protection described herein apply.

3.5 Deletion of data

There is a standard process for deleting personal information, adherence to which is assessed by both the IT administrator as well as the responsible key account manager. Protective Class P4 as per DIN 66399 applies to the destruction of physical data.

3.6 Separation control

There is a separation of productive, testing/development, and administration systems. Database rights have been defined and there is a logical separation of clients in the software. In addition, all accounts are separated by their workload. Storage, Compute, Network is independently handled for every account.

4. Integrity

Access to the databases of the productive systems is logged and saved for twelve (12) months.

5. Availability

5.1 Ensuring availability

A disaster recovery plan is available. We have a business continuity management plan in place. This is described in a business continuity

management policy which is based on ISO 22301:2019 Business Continuity Management to maintain continuity of business process to operational status based on Minimum Business Continuity Output (MBCO). In addition, we use multiple availability zones within our cloud architecture. which ensures uptime also during an outage of a complete datacenter. Data is backed up on a daily basis. All applications are containerized and can be rebuild and deployed on demand.

5.2 Purpose limitation

There are order-specific data processing contracts with all service providers. All employees of the Contractor are continuously and comprehensively trained (seminars, e-learning, and interactive formats like quizzes) on the data protection requirements as well as fundamental information security topics.

6. Durability of systems

The productive systems and servers are continuously monitored by the service provider (see Annex 2) in order to ensure constant availability.

7. Reproduction following incident

The servers and productive systems are continuously ensured every day via full back-up. The back-ups are encrypted and stored on separate server systems of the service provider. Access is granted to the Contractor's administrators. Each back-up is stored for 30 days.

8. Regular assessment of technical and organizational measures

An employee of the Contractor is appointed to be responsible for incident response management. For purposes of continuous improvement of the Contractor's information security, the technical and organizational measures for ensuring data protection and data security are continuously monitored, examined, and improved by the Contractor's management.

Bijlage 2 – Goedgekeurde 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.

Annex 2 – Approved subcontractors

Amazon Web Services EMEA SARL
(Amazon Web Services, Inc. as the contractual party of the EU standard contractual clauses)
38 avenue John F. Kennedy, L-1855, Luxemburg

Hosting of all current and future components required for service provision, including API interface, database system as well as mail server for phishing simulation. We have taken the following measures to protect the data:

- Storage and processing of all data in certified data centers in Germany (Frankfurt a.M.).
- Encryption of all customer data using a master key generated by Processor, so that neither AWS nor any other third party can access customer data, either inside or outside the EU / EEA.
- Conclusion of a data processing agreement as well as the conclusion of the EU standard contractual clauses ((EU) 2021/915, 4.6.2021, module 2 and 3), incl. numerous obligations of AWS on handling and transparency in case of potential authority requests.
- Transfer Impact Assessment (TIA) conducted by an external data protection expert.

- 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:

- Data protection expert opinion on Processor's use of AWS, which can be provided upon request.

Hetzner Online GmbH
Industriestr. 25, 91710 Gunzenhausen

Use of mail services for the Phishing Simulation from SoSafe GmbH. If explicitly agreed with the Controller individually: Provision of the API interface.

ISO27001 certificate for datacenters: https://www.hetzner.de/pdf/FOX_Zertifikat.pdf

salesforce.com Germany GmbH
Mail: Salesforce.com Sarl, Route de la Longeraie 9, Morges, 1110, Switzerland, attn: Director, EMEA Sales Operations, Legal Department: Erika-Mann-Strasse 31-37, 80636, Munich, Germany

Provision of support software (Customer Service Cloud) for customer service (support form or e-mail to support@sosafe.de). This provider is only relevant for the Controller if the Controller uses SoSafe's customer support.

More information: https://trust.salesforce.com/

ISO27001 certificate can be accessed here: https://compliance.salesforce.com/en/iso-27017. In addition, the following measures have been taken:

- 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:

- Storage and processing of all data in certified data centers in Germany (Frankfurt a.M.).
- Encryption of all data with industry-standard encryption products during transfers as well as at rest.
- Conclusion of a data processing agreement incorporating the approved Binding Corporate Rules (BCR) concluded by Salesforce for its group companies and subcontractors as well as the 2021 EU standard contractual clauses with numerous obligations vis-à-vis the competent supervisory authority as well as further voluntary commitments.
- Transfer Impact Assessment (TIA) conducted by an external data protection expert.

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

Provision of an e-mail server infrastructure for customer communication in support cases via the support software (support form or e-mail to support@sosafe.de). This provider is only relevant to the Controller if the Controller uses SoSafe's customer support. The following measures have been taken:

- 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:

- All data are processed and stored exclusively within the European Union as part of the Azure EU Cloud.
- All datacenters are ISO27001- and ISO27018-certified: https://docs.microsoft.com/de-de/azure/security/fundamentals/infrastructure.
- Encryption of all data using industry-standard encryption products during transfers as well as at rest.
- Implementation of the Customer Lockbox, which ensures that Microsoft cannot access content without the Processor's explicit consent.
- Conclusion of a data processing agreement as well as conclusion of the EU standard contractual clauses ((EU) 2021/915, 4.6.2021, module 2 and 3).
- Transfer Impact Assessment (TIA) conducted by an external data protection expert.

Kombo Technologies GmbH (Optional)
Lohmühlenstraße 65, 12435 Berlin, Germany

Integration of Client Active Directory. This provider is only required to the extent that the Client requests Active Directory integration for automated uploading and regular updating of end-user data on the Contractor platform. The following measures have been taken:

- 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.

- All data are processed and stored exclusively within the European Union. Server hosting provider: Google Cloud EMEA Limited.
- Kombo Technologies GmbH is ISO27001 certified. Access can be requested here: https://security.kombo.dev/?itemUid=1fed9faa-4a87-427c-9a95-96b4d6bf66b7&source=click/. More information about Technical and Organizational Security Measures of Kombo Technologies GmbH can be found at security.kombo.dev.
- Encryption
  - All customer data is encrypted using symmetric AES-256 encryption at rest, including backup copies.
  - Data in transit: All outgoing traffic (to integration APIs) uses the highest TLS version available by the respective integration's API (e.g., Google Workspace). All incoming traffic via the Kombo API is enforced to use TLS 1.3. Connections from Kombo's application workloads to Kombo's database also use TLS 1.3 with an AES-256 cipher.
- Conclusion of a data processing agreement.

Bijlage 3 – Personen die bevoegd zijn om instructies te geven

De volgende personen zijn bevoegd om instructies te geven en te ontvangen.

Annex 3 – Persons authorized to issue instructions

The following persons are authorized to issue and receive instructions.

KANT VAN DE OPDRACHTGEVER / CLIENT SIDE:	**KANT VAN DE OPDRACHTNEMER /CONTRACTOR SIDE:**
Raad van bestuur of directie / Board of directors or management	Felix Schürholz, Directeur / Managing Director
Andere door de Opdrachtgever specifiek genoemde personen (bijv. functionarissen voor gegevensbescherming) / Other persons explicitly named by the Client (e.g., data protection officers)	Lukas Schaefer, Directeur / Managing Director
	Dr. Niklas Hellemann, Directeur / Managing Director
	Felix Fichtl, Directeur / Managing Director

SoSafe GmbH | **Lichtstr. 25a | D-50825 Keulen, | Directeuren: Dr. Niklas Hellemann,**
Lukas Schaefer, Felix Schürholz, Felix Fichtl | HRB96220 | *Amtsgericht* Keulen | BTW-nummer: DE322382415 |
Bezoekersadres en parkeerplaats: **Lichtstr. 25a | D-50825 Keulen, | Tel.: +49 (0) 221 6508 3800 |**
E-mailadres: info@sosafe.de | Website: sosafe.de