DATA PRO CREATED BY NEDERLAND ICT

korenter

STANDAARD VERWERKERS-OVEREENKOMST

Deel 1. Data Pro Statement

Deel 2. Standaardclausules voor verwerkingen

De Ondergetekenden

I. Korenter, een besloten vennootschap met beperkte aansprakelijkheid, gevestigd aan het adres Appelgaarde 30 3992 JG Houten hierbij rechtsgeldig vertegenwoordigd door Joeri Noort, hierna te noemen 'Data processor';

en

II. [KLANT] met

KVK-nummer

Adres [ADRES]

Postcode [POSTCODE]

Plaats [PLAATS]

hierbij rechtsgeldig vertegenwoordigd door [VERTEGENWOORDIGER]

hierna te noemen 'Verwerkingsverantwoordelijke'; en tevens 'Opdrachtgever'

hierna tevens afzonderlijk te noemen: 'Partij', en gezamenlijk te noemen: 'Partijen';
zijn op datum van ondertekening deze Verwerkersovereenkomst aangegaan.

Overwegingen

a. Verantwoordelijke en Data processor zijn een ('Overeenkomst') aangegaan. Uit de Overeenkomst vloeit voort dat Data processor Korenter levert aan Verwerkingsverantwoordelijke. Voor de dienstverlening is het noodzakelijk dat Data processor in opdracht van Verwerkingsverantwoordelijke Persoonsgegevens Verwerkt. In Bijlage 1 hebben Partijen de aard van de persoonsgegevens in kwestie en de categorieën betrokkenen nader gespecificeerd.
b. In overeenstemming met de AVG zijn Partijen verplicht om in een Verwerkersovereenkomst nadere afspraken te maken over de Verwerkingen die plaatsvinden.
c. Partijen wensen in deze Verwerkersovereenkomst de afspraken over de Verwerking van Persoonsgegevens in het kader van de diensten vast te leggen.

Aldus overeengekomen en ondertekend door akkoord te gaan met de voorwaarden.

DEEL 1: DATA PRO STATEMENT

Dit Data Pro Statement[1] vormt samen met de Standaardclausules voor verwerkingen de verwerkersovereenkomst[2] voor het product of de dienst van het bedrijf dat dit Data Pro Statement heeft opgesteld.

ALGEMENE INFORMATIE

1. **Dit Data Pro Statement is opgesteld door:**

   Korenter

   Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met:

   Joeri Noort
   Managing Partner
   Email: info@korenter.nl
   Telefoonnummer: 030 - 231 61 32

2. **Dit Data Pro Statement geldt vanaf 15 april 2019**

   De in dit Data Pro Statement omschreven beveiligingsmaatregelen passen wij regelmatig aan om ten aanzien van dataprotectie steeds voorbereid en actueel te blijven. Data Processor[3] houdt u op de hoogte van nieuwe versies via de normale kanalen.

3. **Dit Data Pro Statement is van toepassing op de volgende producten en diensten van data processor**
   - Korenter

4. **Omschrijving Korenter**

   Korenter is een SAAS oplossing voor ledenadministraties, verenigingen, non-profits,

[1] statement van Data Processor waarin hij onder andere informatie geeft met betrekking tot het beoogd gebruik van zijn product of dienst, getroffen beveiligingsmaatregelen, subverwerkers, datalekken, certificeringen en omgang met rechten van Data subjects.
[2] de Standaardclausules voor verwerkingen, die tezamen met het Data Pro Statement (of vergelijkbare informatie) van Data Processor de verwerkersovereenkomst vormen als bedoeld in artikel 28, lid 3 Avg.
[3] partij die als ICT-leverancier in het kader van de uitvoering van de Overeenkomst als verwerker Persoonsgegevens verwerkt ten behoeve van diens Opdrachtgever.

stichtingen, op het gebied van relatiebeheer, ledenadministratie en dienstverlening. Het aantal data subjects[4] is ongeveer 500.000.

De dienst is doorgaans essentieel voor de klant om hun dagelijkse taken te kunnen verrichten. Een beperkt aantal medewerkers van **Korenter** kunnen in principe bij alle gegevens van klanten tbv onderhoud en support. Zij zullen, tenzij anders afgesproken, geen persoonsgegevens[5] wijzigen of toevoegen, maar slechts inzien om een technisch probleem op te lossen.

5. **Beoogd gebruik**
   Korenter is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:

   Deze software is **niet** bedoeld om bijzondere gegevens mee te verwerken: medische gegevens, genetische gegevens met het oog op de unieke identificatie van een persoon, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens waaruit ras of etnische afkomst blijkt, gegevens waaruit politieke opvattingen blijken, gegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken, gegevens waaruit het lidmaatschap van een vakbond blijkt, gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten zoals beschreven in artikel 10 van het AVG[6] en door het beroepsgeheim beschermde persoonsgegevens. Deze software is expliciet **niet** bedoeld om gegevens die over het algemeen beschouwd kunnen worden als een verhoging van het mogelijke risico met betrekking tot de rechten en vrijheden van personen.

   - electronic communication data
   - location data
   - financial data
   - Informatie die door een natuurlijke persoon wordt verwerkt in de context van puur persoonlijke of huishoudelijke activiteiten waarvan de openbaarmaking of de verwerking voor enig andere doeleinden dan huishoudelijke activiteiten als heel intrusief kan worden beschouwd

   Als de Verwerkingsverantwoordelijke het als doel heeft om toch een van deze categorieën bijzondere persoonsgegevens te registreren moeten daar specifiek afspraken over worden gemaakt met **Korenter** en zijn er mogelijk extra kosten verbonden hieraan.

[4] een geïdentificeerde of identificeerbare natuurlijke persoon.
[5] alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals omschreven in artikel 4, sub 1 Avg, die Data Processor in het kader van de uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst verwerkt.
[6] de Algemene verordening gegevensbescherming.

Verwerken van deze gegevens met het hiervoor omschreven product of dienst door opdrachtgever[7] is ter eigen beoordeling door opdrachtgever.

6. **Data processor heeft bij het ontwerpen van het product/de dienst *privacy by design* op de volgende wijze toegepast:**

- Data processor heeft een speciale GDPR / AVG tool ontwikkeld waarmee het mogelijk is voor Verwerkingsverantwoordelijken met oog op het recht op inzage en dataportabiliteit. Er kan voor een relatie een machine leesbaar bestand worden aangemaakt door de software bij een relatie als een data subject zich beroept op het recht op dataportabiliteit. Dit is tevens ook behulpzaam bij het inzage verlenen aan een data subject. Hier zijn wel extra licentiekosten aan verbonden.
- Twee-weg authenticatie by default.
- Bij het aanmaken van nieuwe autorisatierollen door de systeembeheerder moeten permissies actief verleend worden. Alle toestemmingen staan standaard op “geen toegang”.
- Autorisatiesysteem: er kunnen verschillende autorisatierollen met diverse permissies worden aangemaakt per module.
- Het is mogelijk om een groep gebruikers vrij gedetailleerd toegang te geven of te weigeren tot bepaalde gedeeltes met bijzondere persoonsgegevens.
- De software waarschuwt actief bij het toekennen van permissies in het autorisatie menu met toegang tot zowel bedrijfskritieke processen zoals bulk mailingen, incasso’s, en facturatie en privacy gevoelige gebieden in de software zoals dossier, medische gegevens en meer. Verwerkingsverantwoordelijke is zelf verantwoordelijk voor het juiste gebruik van dit systeem.
- Bij het verwijderen van inactieve relaties in bulk staat de software zo ingesteld dat het standaard alle inactieve relaties zal selecteren uit de door de Verwerkingsverantwoordelijke geselecteerde periode ivm het recht op vergetelheid. Er kan wel voor worden gekozen worden om alleen relaties die om een bepaalde reden inactief zijn gezet te selecteren eventueel vanaf een specifieke datum maart dit moet actief ingesteld worden door de Verwerkingsverantwoordelijke.
- Bij het verwijderen van inactieve relaties staat standaard ingesteld dat alle inactieve relaties van tot 2 jaar terug worden meegenomen. De gebruiker kan dit uiteraard dan nog aanpassen naar eigen inzicht. en bijvoorbeeld alleen gebruikers die om een specifieke reden inactief zijn worden verwijderd.

7. **Backups worden maximaal 2 maanden bewaard.**

[7] partij in wiens opdracht Data Processor persoonsgegevens verwerkt. De Opdrachtgever kan zowel Verwerkingsverantwoordelijke (“controller”) zijn als een andere verwerker.

8. **Data processor gebruikt de Data Pro Standaardclausules voor verwerkingen, welke in het tweede gedeelte van dit document is opgenomen.**

9. **Data processor verwerkt de persoonsgegevens van zijn opdrachtgevers (data subjects) uitsluitend binnen Nederland en daarmee binnen de EU als het gaat om de persoonsgegevens van data subjects.**
   Incidenteel kan het voorkomen dat gegevens van gebruikers (zoals medewerkers van de Verwerkingsverantwoordelijke) van Korenter (tijdelijk) buiten de EU/EER verwerkt worden als er persoonsgegevens door de Verwerkingsverantwoordelijke naar Data Processor toe worden verzonden. De data zal in dat geval uitsluitend verwerkt worden bij sub-verwerkers die bij Privacy Shield zijn aangesloten.

10. **Data processor maakt gebruik van de volgende sub-verwerkers als het gaat om de persoonsgegevens en overige data van data subjects / betrokkenen (de relaties en klanten van de klanten van Data Processor in hun rol als Verwerkingsverantwoordelijke) maakt data processor gebruik van de volgende sub-verwerkers:**

    Korenter heeft gekozen voor de datacentra van TransIP. TransIP heeft de beschikking over een eigen ruimte in datacenter DCG (The Datacenter Group Amsterdam). De servers van Data Processor worden onderhouden door Robuust Computer Solutions.

    Indien gebruik gemaakt wordt van het systeem Te Veel Papier is Mailcamp b.v. ook een sub-verwerker. De sub-verwerkers van Mailcamp ivm het hosten van de data is Exsilia Internet b.v.

    Indien er gebruik gemaakt wordt van de koppeling van Mollie voor iDeal is Mollie in principe een sub-verwerker van de data, echter moet de Verwerkingsverantwoordelijke zelf een Mollie account moet aanmaken om gebruik te kunnen maken van deze dienst. Hierdoor moet de Verwerkingsverantwoordelijke zelf afspraken rechtstreeks met Mollie te maken mbt tot privacy en security en zal Mollie ook rechtstreeks een rol als verwerker (Contract, verwerkersovereenkomst etc.) vervullen richting de Verwerkingsverantwoordelijke.

11. **Ten bate van contact voor support, onderhoud en algemene service voor de Verwerkingsverantwoordelijke maakt data processor gebruik van de volgende sub-verwerkers. Data processor slaat geen gegevens van datasubjecten (de relaties en klanten van de klanten van Data Processor in hun rol als Verwerkingsverantwoordelijke) op bij de onderstaande sub-verwerkers. Hierin slaan we tevens geen bijzondere persoonsgegevens op.**

    Mail tbv support en onderhoud van **Korenter** gebruikers (medewerkers van de

Verwerkingsverantwoordelijke) maakt data processor gebruik van Gsuite (Google LLC) als sub-verwerker. Google LLC is aangesloten bij Privacy Shield.
Voor contact als het gaat om projecten maakt data processor incidenteel gebruik van Trello (Atlassian PTY Ltd). Atlassian PTY Ltd is aangesloten bij Privacy Shield. Voor het verwerken van financiële gegevens tbv boekhouding is Reeleezee b.v. sub processor.

12. **Data processor ondersteunt klanten op de volgende manier bij verzoeken van betrokkenen:**

    In **Korenter** is het mogelijk om zelf gegevens van data subjects / betrokkenen te verwijderen als een verzoek hiertoe binnenkomt.

    De AVG tool vormt een uitbreiding hierop speciaal gericht op dataportabilieit en recht op inzage. Hiermee kun je alle mogelijke gegevens die bekend zijn over een betrokkene in de software in ZIP bestand beschikbaar stellen. Nadat de software het ZIP bestand heeft gegenereerd is deze te downloaden uit **Korenter** en op een eigen (beveiligde) wijze aan te leveren aan de betrokkenen. In het ZIP bestand zitten de gegevens van de betrokkene als XML bestand, waarmee het voldoet aan de eis dat het bestand door een computer leesbaar moet zijn en daarnaast ook als Docx bestand zodat het goed leesbaar is voor de klant. Aan het gebruik van deze tool zijn (extra) kosten verbonden.

13. **Na beëindiging van de overeenkomst[8] met een opdrachtgever verwijdert data processor de persoonsgegevens die hij voor opdrachtgever verwerkt binnen 3 maanden. Data processor streeft ernaar om de data binnen 10 werkdagen te verwijderen.**

14. **Na beëindiging van de overeenkomst met opdrachtgever retourneert data processor alle persoonsgegevens die hij voor opdrachtgever verwerkt binnen 3 maanden op de volgende manier:**

    Bij beëindiging van de overeenkomst en daarmee de verwerkersovereenkomst, of indien van toepassing aan het einde van de overeengekomen bewaartermijnen, of op schriftelijk verzoek van opdrachtgever zal **Korenter**, kosteloos, naar keuze van opdrachtgever, de persoonsgegevens vernietigen of teruggeven aan opdrachtgever. Teruggave zal plaatsvinden binnen 3 maanden na het beëindigen van den overeenkomst. Op verzoek van opdrachtgever verstrekt **Korenter** bewijs van het feit dat de gegevens vernietigd of verwijderd zijn. Bij teruggave van de persoonsgegevens zal de aanlevering gebeuren via een standaard database MySQL backup-bestand. Op

[8] De tussen Opdrachtgever en Data Processor geldende overeenkomst, op basis waarvan de ICT-leverancier diensten en/of producten levert aan Opdrachtgever, waarvan de verwerkersovereenkomst onderdeel vormt.

verzoek kunnen de persoonsgegevens ook in een andere format worden teruggegeven, echter zijn hier kosten aan verbonden.

Beveiligingsbeleid

15. **Data processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:**

Datacentrum & hosting

Korenter wordt uitsluitend gehost vanuit datacentra op private dedicated servers die zich in Nederland bevinden en welke uitsluitend via de eerdergenoemde beveiligde procedures te benaderen zijn. Korenter heeft gekozen voor de datacentra van TransIP en deze is hiermee subverwerker van de klantdata. TransIP heeft de beschikking over een eigen ruimte in datacenter DCG (The Datacenter Group Amsterdam). De fysieke locatie is Kabelweg 48a, 1014 BB Amsterdam. Het datacentrum is ISO 9001, ISO 27001, ISO 14001, NEN 7510 en PCI DDS gecertificeerd. Daarmee zijn kwaliteitsmanagement, beveiliging en milieumanagement optimaal gewaarborgd. De servers zelf bevinden zich in een afgesloten ruimte, waar slechts een select aantal medewerkers toegang toe hebben. Het datacentrum beschikt over 24/7 on-site bewaking. Biometrische identificatie en een HD CCTV netwerk waarborgen dat de server veilig staat. Brandveiligheid wordt gegarandeerd door een VESDA detectiesysteem in combinatie met een Argonite blussysteem. Alle racks in het datacentrum zijn voorzien van redundante netwerkpoorten. Een Uninterruptible Power Supply (UPS) en twee SDMO NSA dieselgeneratoren zorgen ervoor dat zelfs bij stroomuitval het datacentrum volledig operationeel blijft. Er worden iedere 4 uur offsite backups van de data gemaakt naar een datacenter op een andere locatie (Heertjeslaan 1, 2629 JG Delft). De datacentra vallen onder Nederlandse wet- en regelgeving Gebruikers kunnen namens de verwerkingsverantwoordelijke alleen toegang krijgen tot de software via een beveiligde SSL-verbinding. Hierdoor wordt de mogelijkheid van ‘afluisteren’ door derden geëlimineerd. Gebruikers kunnen enkel inloggen via een twee-weg authenticatie welke gebruik maakt van de e-mailaccount van de gebruiker. Derden zouden zowel de login gegevens van de **Korenter** gebruiker als de accountgegevens van de e-mail account van gebruiker moeten bemachtigen.
Vanuit ons beleid raden wij klanten het ten strengste af om e-mails met persoonsgegevens erin op te sturen omdat dit onveilig is. Mocht er een probleem zijn in de software dan vragen medewerkers van Data Processor indien nodig om een relatienummer van een betrokkene in de software waarna medewerkers op beveiligde wijze kunnen inloggen om onderhoud en support te verrichten. Het kan wel voorkomen dat Data Processor data toegestuurd krijgen door een klant en vanuit het beleid van Data Processor mag dit uitsluitend door gebruik van SFTP of een vergelijkbaar goed beveiligde verzendwijze.

Isolatie van gegevens
De gegevens van de Verwerkingsverantwoordelijke zijn binnen de infrastructuur van **Korenter** geïsoleerd. De database waar de gegevens in worden opgeslagen is niet direct via internet toegankelijk en kan alleen via de **Korenter** software worden benaderd. De documenten en dossiers in de software zijn niet direct toegankelijk, waardoor eventuele virussen op het netwerk van een gebruiker niet zelfstandig kunnen propageren naar de desbetreffende documenten in de software.

Virussen
De Verwerkingsverantwoordelijke dient zelf zorg te dragen voor een toereikende virusscanner op haar eigen systeem. **Korenter** kan niet voorkomen dat door het gebruik van een geïnfecteerd systeem, gegevens worden blootgesteld aan derden, of dat bestanden welke in **Korenter** worden opgeslagen, het virus bij zich dragen. **Korenter** draagt er zorg voor dat eventuele virussen afkomstig uit het netwerk van de gebruiker, niet kunnen propageren binnen de instantie van **Korenter**, of tussen verschillende instanties van **Korenter**.

Medewerkers van Korenter
Alle medewerkers van **Korenter** die toegang hebben tot vertrouwelijke gegevens zijn contractueel verplicht om correct en vertrouwelijk met alle gegevens van de Verwerkingsverantwoordelijke om te gaan. Alle medewerkers als ook eventueel ingehuurde krachten hebben een geheimhoudingsverklaring getekend. Dit betreft alle communicatie met de Verwerkingsverantwoordelijke en indien van toepassing, de persoonsgegevens van de klanten in de database. Een beperkt aantal medewerkers van **Korenter** heeft toegang tot de software en de persoonsgegevens van klanten. Deze toegang wordt uitsluitend gebruikt voor het leveren van support en onderhoud aan de software en servers en uitdrukkelijk niet voor het wijzigen van gegevens.
Medewerkers kunnen alleen toegang krijgen tot de software vanuit de werklocaties via een beveiligde digitale sleutel. Hierdoor is zelfs in het geval dat het wachtwoord bij derden terecht komt, niet mogelijk dat hier direct misbruik van gemaakt wordt; het wachtwoord geeft alleen op de werklocatie en met gelijktijdig gebruik van de unieke digitale sleutel toegang tot het systeem. De computers waarmee ingelogd wordt om onderhoud en support te verlenen zijn encrypted.

Extra kosten
Extra technische en organisatorische maatregelen op maat zijn mogelijk maar daar zijn extra kosten aan verbonden die door de Verwerkingsverantwoordelijke, de klant gedragen moeten worden.

Behoud persoonsgegevens

De Verwerkingsverantwoordelijke is zelf verantwoordelijk voor het verwijderen van persoonsgegevens van oud klanten na de voor hen geldende maximale bewaarperiode. Er zijn functies beschikbaar welke het verwijderen van de oude gegevens (in bulk) kunnen faciliteren.

Melding beveiligingsincidenten
Data processor zal zich inspannen de hieronder nader uitgewerkte beveiligingsincidenten te melden aan Klant:

- Aanhoudende verdachte inlogpogingen (specificeren: locatie, IP-nummers, tijdstippen)
- Bij een DDOS (Distributed Denial of Service) aanval
- Daadwerkelijke datalekken
- Onbevoegde on site fysieke toegang tot het systeem

Opdrachtnemer heeft in het kader van het melden van beveiligingsincidenten de volgende maatregelen getroffen:

Bij aanhoudende verdachte inlogpogingen wordt toegang tot het systeem voor iedereen geblokkeerd en wordt de Data processor gealarmeerd. De verdachte inlogpogingen worden geanalyseerd en gemeld bij de Verwerkingsverantwoordelijke als de aard hiervan een direct gevaar vormt of verdacht blijft. Verdachte inlogpogingen worden geanalyseerd op maandelijkse basis.

16. **Data processor is Data Pro Code compliant. Zodra de Data Pro Code certificering beschikbaar is zullen wij ons laten certificeren. Ieder jaar zal dit opnieuw worden getoetst door een onafhankelijke partij.**

Datalekprotocol

17. **In geval er toch iets mis gaat, hanteert data processor het volgende datalekprotocol om ervoor te zorgen dat klanten op de hoogte zijn van incidenten.**

Stap 1: Constateren van een datalek
Er is sprake van een 'inbreuk in verband met persoonsgegevens' (hierna: **datalek**) als er een **inbreuk is op de beveiliging die** als gevolg of mogelijk gevolg heeft:

- **vernietiging** van persoonsgegevens (bijvoorbeeld door brand of wissen); **of**
- **verlies** van persoonsgegevens (bijvoorbeeld USB of laptop die kwijtraakt); **of**
- **wijziging** van persoonsgegevens (zonder dat dit de bedoeling was); **of**
- ongeoorloofde **verstrekking** van persoonsgegevens (bijvoorbeeld e-mail/bestanden verzonden aan verkeerde geadresseerde of onbedoelde CC's); **of**
- ongeoorloofde **toegang** tot doorgezonden/opgeslagen/anderszins verwerkte persoonsgegevens (bijvoorbeeld door een hacker of een niet-bevoegd personeelslid).

Het maakt daarbij niet uit of sprake is van een **opzettelijk** datalek (zoals een hacker die zich ongeoorloofd toegang verschaft tot persoonsgegevens) of dat er **per ongeluk** iets mis gaat

(bijvoorbeeld door per ongeluk wissen van gegevens die niet gewist moesten worden). Het maakt wel uit of sprake is van **persoonsgegevens**. Als er geen gevolgen zijn voor persoonsgegevens, is er geen datalek.

Indien een datalek geconstateerd wordt, volgt Data Processor de volgende stappen in dit plan.

Stap 2: Crisisteam

Indien een datalek geconstateerd of vermoed wordt vormen de volgende personen het crisisteam. Het team bevat – zo mogelijk – de volgende expertise:

- ICT Specialist: Joeri Noort (Directie)
- Server beheerder: ROBUUST Computer Solutions
- Data Protection Officer: Maarten Bakker

Eventueel en indien noodzakelijk zal deze team worden aangevuld met:

- Jurist
- Verzekeraar

Stap 3: Maatregelen om het (actieve) lek te stoppen of de gevolgen te beperken

In het geval er een datalek wordt geconstateerd, draagt Korenter zorg om de schade te beperken. Indien data processor een datalek constateert zullen zal dataprocessor hier actie op ondernemen door het gedeeltelijk of geheel blokkeren van toegang tot de software. In overleg kan op een later tijdstip de toegang weer gedeeltelijk hersteld worden. Ook zal de betrokken Verwerkingsverantwoordelijke binnen 24 uur na het ontdekken van de datalek worden ingelicht over het datalek en de status van het onderzoek hiernaar.
Andere mogelijke acties ter beperking van de schade en stoppen van het datalek zijn na het constateren van het datalek zijn:

- Blokkeren van alle netwerkverkeer naar de servers
- Beperkt openstellen van netwerkverkeer naar de server voor analyse
- Het wijzigen van beheer- en onderhoudswachtwoorden
- Verplaatsen van data naar een veilige locatie
- Formatteren/herinstalleren systeem
- Zoeken (bijvoorbeeld bij kwijtgeraakte USB-stick of harde schijf)
- Remote wipe (bijvoorbeeld bij gestolen laptop)

Van alle belangrijke constateringen en genomen stappen zal Data Processor een log bijhouden.

Stap 4: Verzameling van informatie

1. Wat is het voor incident (kies er 1):

- Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens kwijtgeraakt of gestolen;
- Brief of postpakket met persoonsgegevens kwijtgeraakt of geopend retour ontvangen;
- Hacking, malware (bijv. ransomware) en/of phishing;
- Persoonsgegevens bij oud papier gezet;
- Persoonsgegevens nog aanwezig op afgedankt apparaat of op afgedankte gegevensdrager (bijv. USB-stick);
- Persoonsgegevens per ongeluk gepubliceerd;
- Persoonsgegevens van verkeerde klant getoond in klantportaal; -
- Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger.
- Overig;

2. *Geef een samenvatting van het incident:*

   <samenvatting>

3. *Indien het incident plaatsvond bij een sub-verwerker:*

   <naam subverwerker>

4. Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

- Minimaal: <vul aantal in>
- Maximaal: <vul aantal in>

5. Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk:

- <bijvoorbeeld: / patiënten van ziekenhuis X / klanten van webwinkel Y / leerlingen van basisscholen in regio Z / 60+ers in NoordNederland / etc. >

6. Wanneer vond de inbreuk plaats? (kies 1 optie en vul zo nodig aan)

- Op (datum)
- Tussen (begindatum) en (einddatum)
    - Nog niet bekend

7. Wat is de aard van de inbreuk? (meerdere opties mogelijk)

- Lezen (vertrouwelijkheid)
- Kopiëren
- Veranderen (integriteit)
- Verwijderen of vernietigen (beschikbaarheid)
- Diefstal
- Nog niet bekend
- Anders: <vul in>

8. Om welk type persoonsgegevens gaat het? (meerdere opties mogelijk)

- Naam-, adres en woonplaatsgegevens
- Telefoonnummers
- E-mailadressen of andere adressen voor elektronische communicatie
- Toegangs- of identificatiegegevens
- Financiële gegevens
- Burgerservicenummer (BSN)
- Paspoortkopieën of kopieën van andere legitimatiebewijzen
- Geslacht, geboortedatum en/of leeftijd
- Zorggegevens
- Diploma's
- Anders nl:

Persoonsgegevens met informatie over

- Ras of etnische afkomst
- Politieke opvattingen
- Religieuze of levensbeschouwelijke overtuigingen
- Lidmaatschap van een vakbond
- Genetische gegevens
- Biometrische gegevens met het oog op unieke identificatie van een persoon
- Gezondheid
- Iemands seksueel gedrag of seksuele gerichtheid
- Strafrechtelijke veroordelingen of strafrechtelijke feiten

- Onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag
- iemands godsdienst of levensovertuiging
- overige, <toelichting>
- onbekend

Toelichting:

<toelichting indien van toepassing>

Stap 5: Informeren Verwerkingsverantwoordelijke

Indien Verwerkingsverantwoordelijke over een Data Protection Officer / Functionaris van de Gegevensbescherming beschikt zal de melding tenzij anders is afgesproken bij deze gemeld worden als contactpersoon. In overleg kan door de Verwerkingsverantwoordelijke (ook) een contactpersoon worden aangewezen welke ook buiten kantoortijden beschikbaar is. Als er geen contactpersoon is aangewezen of de contactpersoon niet bereikbaar is, zal **Korenter** zich inspannen om een Verantwoordelijke binnen de organisatie van de Verwerkingsverantwoordelijke te bereiken via telefoon of e-mail. De Verwerkingsverantwoordelijke is zelf verantwoordelijk voor het melden bij het Autoriteit Persoonsgegevens (AP)[9] van het datalek.

Een datalek zal per email met het onderwerp: “datalek melding” worden gemeld bij de contactpersoon van de Klant via het door de klant aangedragen emailadres.

Contactgegevens van contactpersoon 2 van Verwerkingsverantwoordelijke:

Naam:

Emailadres:

Telefoonnummer:

Inhoud van de melding:

In de melding zullen de gegevens worden vermeld die in Stap 5 zijn verzameld:

Contactpersonen Korenter

[9] toezichthoudende autoriteit, zoals omschreven in artikel 4, sub 21 Avg.

De contactpersoon vanuit Korenter is Joeri Noort, bereikbaar per mail: info@korenter.nl en telefonisch: 030 - 23 161 32

Data Protection Officer is Maarten Bakker bereikbaar per mail: dpo@koren.nl en telefonisch: 06-10326340

Stap 6: Voorkomen van herhaling in de toekomst

Om herhaling te voorkomen zal er naar aanleiding van het onderzoek naar de datalek eventueel stappen genomen worden om te voorkomen dat het datalek zich nogmaals voordoet.

Deel 2: Standaardclausules voor verwerkingen

versie: april 2018

Artikel 1. Definities

Onderstaande begrippen hebben in deze Standaardclausules voor verwerkingen, in het Data Pro Statement en in de Overeenkomst de volgende betekenis:

1.1 **Autoriteit Persoonsgegevens (AP):** toezichthoudende autoriteit, zoals omschreven in artikel 4, sub 21 Avg.

1.2 **Avg:** de Algemene verordening gegevensbescherming ook bekend als GDPR (General Data Protection Regulation)

1.3 **Data Processor (verwerker)**: Partij die als ICT-leverancier in het kader van de uitvoering van de Overeenkomst als verwerker Persoonsgegevens verwerkt ten behoeve van diens Opdrachtgever.

1.4 **Data Pro Statement**: statement van Data Processor waarin hij onder andere informatie geeft met betrekking tot het beoogd gebruik van zijn product of dienst, getroffen beveiligingsmaatregelen, subverwerkers, datalekken, certificeringen en omgang met rechten van Data subjects.

1.5 **Data subject (betrokkene)**: een geïdentificeerde of identificeerbare natuurlijke persoon.

1.6 **Opdrachtgever:** Partij in wiens opdracht Data Processor persoonsgegevens verwerkt. De Opdrachtgever kan zowel Verwerkingsverantwoordelijke (“controller”) zijn als een andere verwerker.

1.7 **Overeenkomst**: de tussen Opdrachtgever en Data Processor geldende overeenkomst, op basis waarvan de ICT-leverancier diensten en/of producten levert aan Opdrachtgever, waarvan de verwerkersovereenkomst onderdeel vormt.

1.8 **Persoonsgegevens**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals omschreven in artikel 4, sub 1 Avg, die Data Processor in het kader van de uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst verwerkt.

1.9 **Verwerkersovereenkomst**: deze Standaardclausules voor verwerkingen, die tezamen met het Data Pro Statement (of vergelijkbare informatie) van Data Processor de verwerkersovereenkomst vormen als bedoeld in artikel 28, lid 3 Avg.

Artikel 2. Algemeen

2.1 Deze Standaardclausules voor verwerkingen zijn van toepassing op alle verwerkingen van Persoonsgegevens die Data Processor doet in het kader van de levering van zijn producten en diensten en op alle Overeenkomsten en aanbiedingen. De toepasselijkheid

van verwerkersovereenkomsten van Opdrachtgever wordt uitdrukkelijk van de hand gewezen.

2.2 Het Data Pro Statement, en met name de daarin opgenomen beveiligingsmaatregelen, kan van tijd tot tijd door Data Processor worden aangepast aan veranderende omstandigheden. Data Processor zal Opdrachtgever van significante aanpassingen op de hoogte stellen. Indien Opdrachtgever in redelijkheid niet akkoord kan gaan met de aanpassingen, is Opdrachtgever gerechtigd binnen 30 dagen na kennisgeving van de aanpassingen de verwerkersovereenkomst schriftelijk gemotiveerd op te zeggen.

2.3 Data Processor verwerkt de Persoonsgegevens namens en in opdracht van Opdrachtgever overeenkomstig de met Data Processor overeengekomen schriftelijke instructies van Opdrachtgever.

2.4 Opdrachtgever, dan wel diens klant, is de Verwerkingsverantwoordelijke in de zin van de Avg, heeft de zeggenschap over de verwerking van de Persoonsgegevens en heeft het doel van en de middelen voor de verwerking van de Persoonsgegevens vastgesteld.

2.5 Data Processor is verwerker in de zin van de Avg en heeft daarom geen zeggenschap over het doel van en de middelen voor de verwerking van de Persoonsgegevens en neemt derhalve geen beslissingen over onder meer het gebruik van de Persoonsgegevens.

2.6 Data Processor geeft uitvoering aan de Avg zoals neergelegd in deze Standaardclausules voor verwerkingen, het Data Pro Statement en de Overeenkomst. Het is aan Opdrachtgever om op basis van deze informatie te beoordelen of Data Processor afdoende garanties biedt met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking aan de vereisten van de Avg voldoet en de bescherming van de rechten van Data subjects voldoende zijn gewaarborgd.

2.7 Opdrachtgever staat er tegenover Data Processor voor in dat hij conform de Avg handelt, dat hij zijn systemen en infrastructuur te allen tijde adequaat beveiligt en dat de inhoud, het gebruik en/of de verwerking van de Persoonsgegevens niet onrechtmatig zijn en geen inbreuk maken op enig recht van een derde.

2.8 Een aan Opdrachtgever door de AP opgelegde bestuurlijke boete kan niet worden verhaald op Data Processor, tenzij er sprake is van opzet of bewuste roekeloosheid aan de zijde van de bedrijfsleiding van Data Processor.

Artikel 3. Beveiliging

3.1 Data Processor treft de technische en organisatorische beveiligingsmaatregelen, zoals omschreven in zijn Data Pro Statement. Bij het treffen van de technische en organisatorische beveiligingsmaatregelen heeft Data Processor rekening gehouden met de stand van de techniek, de uitvoeringskosten van de beveiligingsmaatregelen, de aard, omvang en de context van de verwerkingen, de doeleinden en het beoogd gebruik van zijn producten en diensten, de verwerkingsrisico’s en de qua waarschijnlijkheid en ernst uiteenlopende risico’s voor de rechten en vrijheden van Data subjects die hij gezien het beoogd gebruik van zijn producten en diensten mocht verwachten.

3.2 Tenzij expliciet anders vermeld in het Data Pro Statement is het product of de dienst van Data Processor niet ingericht op de verwerking van bijzondere categorieën van Persoonsgegevens of gegevens betreffende strafrechtelijke veroordelingen of strafbare feiten.

3.3 Data Processor streeft ernaar dat de door hem te treffen beveiligingsmaatregelen passend zijn voor het door Data Processor beoogde gebruik van het product of de dienst.

3.4 De omschreven beveiligingsmaatregelen bieden, naar het oordeel van de Opdrachtgever, rekening houdend met de in artikel 3.1 genoemde factoren een op het risico van de verwerking van de door hem gebruikte of verstrekte Persoonsgegevens afgestemd beveiligingsniveau.

3.5 Data Processor kan wijzigingen aanbrengen in de getroffen beveiligingsmaatregelen indien dat naar zijn oordeel noodzakelijk is om een passend beveiligingsniveau te blijven bieden. Data Processor zal belangrijke wijzigingen vastleggen, bijvoorbeeld in een aangepast Data Pro Statement, en zal Opdrachtgever waar relevant van die wijzigingen op de hoogte stellen.

3.6 Opdrachtgever kan Data Processor verzoeken nadere beveiligingsmaatregelen te treffen. Data Processor is niet verplicht om op een dergelijk verzoek wijzigingen door te voeren in zijn beveiligingsmaatregelen. Data Processor kan de kosten verband houdende met de op verzoek van Opdrachtgever doorgevoerde wijzigingen in rekening brengen bij Opdrachtgever. Pas nadat de door Opdrachtgever gewenste gewijzigde beveiligingsmaatregelen schriftelijk zijn overeengekomen en ondertekend door Partijen, heeft Data Processor de verplichting deze beveiligingsmaatregelen daadwerkelijk te implementeren.

Artikel 4. Inbreuken in verband met Persoonsgegevens

4.1 Data Processor staat er niet voor in dat de beveiligingsmaatregelen onder alle omstandigheden doeltreffend zijn. Indien Data Processor een inbreuk in verband met Persoonsgegevens (zoals bedoeld in artikel 4 sub 12 Avg) ontdekt, zal hij Opdrachtgever zonder onredelijke vertraging informeren. In het Data Pro Statement (onder datalekprotocol) is vastgelegd op welke wijze Data Processor Opdrachtgever informeert over inbreuken in verband met Persoonsgegevens.

4.2 Het is aan de Verwerkingsverantwoordelijke (Opdrachtgever, of diens klant) om te beoordelen of de inbreuk in verband met Persoonsgegevens waarover Data Processor heeft geïnformeerd gemeld moet worden aan de AP of Data subject. Het melden van inbreuken in verband met Persoonsgegevens, die op grond van artikel 33 en 34 Avg moeten worden gemeld aan de AP en/of Data subjects, blijft te allen tijde de verantwoordelijkheid van de Verwerkingsverantwoordelijke (Opdrachtgever of diens klant). Data Processor is niet verplicht tot het melden van inbreuken in verband met persoonsgegevens aan de AP en/of de Betrokkene.

4.3 Data Processor zal, indien nodig, nadere informatie verstrekken over de inbreuk in verband met Persoonsgegevens en zal zijn medewerking verlenen aan noodzakelijke informatievoorziening aan Opdrachtgever ten behoeve van een melding als bedoeld in artikel 33 en 34 Avg.

4.4 Data Processor kan de redelijke kosten die hij in dit kader maakt in rekening brengen bij Opdrachtgever tegen zijn dan geldende tarieven.

Artikel 5. Geheimhouding

5.1 Data Processor waarborgt dat de personen die onder zijn verantwoordelijkheid Persoonsgegevens verwerken een geheimhoudingsplicht hebben.

5.2 Data Processor is gerechtigd de Persoonsgegevens te verstrekken aan derden, indien en voor zover verstrekking noodzakelijk is ingevolge een rechterlijke uitspraak, een wettelijk voorschrift of op basis van een bevoegd gegeven bevel van een overheidsinstantie.

5.3 Alle door Data Processor aan Opdrachtgever verstrekte toegangs- en/of identificatiecodes, certificaten, informatie omtrent toegangs- en/of wachtwoordenbeleid en alle door Data Processor aan Opdrachtgever verstrekte informatie die invulling geeft aan de in het Data Pro Statement opgenomen technische en organisatorische beveiligingsmaatregelen zijn vertrouwelijk en zullen door Opdrachtgever als zodanig worden behandeld en slechts aan geautoriseerde medewerkers van Opdrachtgever kenbaar worden gemaakt. Opdrachtgever ziet erop toe dat zijn medewerkers de verplichtingen uit dit artikel naleven.

Artikel 6. Looptijd en beëindiging

6.1 Deze verwerkersovereenkomst maakt onderdeel uit van de Overeenkomst en iedere daaruit voortkomende nieuwe of nadere overeenkomst, treedt in werking op het moment van totstandkoming van de Overeenkomst en wordt gesloten voor onbepaalde tijd.

6.2 Deze verwerkersovereenkomst eindigt van rechtswege bij beëindiging van de Overeenkomst of enige nieuwe of nadere overeenkomst tussen partijen.

6.3 Data Processor zal, in geval van einde van de verwerkersovereenkomst, alle onder zich zijnde en van Opdrachtgever ontvangen Persoonsgegevens binnen de in het Data Pro Statement opgenomen termijn verwijderen op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (*render inaccessible*), of, indien overeengekomen, in een machine leesbaar formaat terugbezorgen Opdrachtgever.

6.4 Data Processor kan eventuele kosten die hij maakt in het kader van het in artikel 6.3 gestelde in rekening brengen bij Opdrachtgever. Hierover kunnen nadere afspraken worden neergelegd in het Data Pro Statement.

6.5 Het bepaalde in artikel 6.3 geldt niet indien een wettelijke regeling het geheel of gedeeltelijk verwijderen of terugbezorgen van de Persoonsgegevens door Data Processor belet. In een dergelijk geval zal Data Processor de Persoonsgegevens enkel blijven verwerken voor zover noodzakelijk uit hoofde van zijn wettelijke verplichtingen. Het bepaalde in artikel 6.3 geldt eveneens niet indien Data Processor

Verwerkingsverantwoordelijke in de zin van de Avg is ten aanzien van de Persoonsgegevens.

Artikel 7. Rechten Data subjects, Data Protection Impact Assessment (DPIA) en Auditrechten

7.1 Data Processor zal, waar mogelijk, zijn medewerking verlenen aan redelijke verzoeken van Opdrachtgever die verband houden met bij Opdrachtgever door Data subjects ingeroepen rechten van Data subjects. Indien Data Processor direct door een Data subject wordt benaderd, zal hij deze waar mogelijk doorverwijzen naar Opdrachtgever.

7.2 Indien Opdrachtgever daartoe verplicht is, zal Data Processor na een daartoe redelijk gegeven verzoek zijn medewerking verlenen aan een gegevensbeschermingseffectbeoordeling (DPIA) of een daarop volgende voorafgaande raadpleging zoals bedoeld in artikel 35 en 36 Avg.

7.3 Data Processor kan de naleving van zijn verplichtingen op grond van de verwerkersovereenkomst aantonen door middel van Data Pro Code compliance (zodra de Data Pro Code certificaat beschikbaar is laten we ons officieel certificeren.

7.4 Data Processor zal daarnaast op verzoek van Opdrachtgever alle verdere informatie ter beschikking stellen die in redelijkheid nodig is om nakoming van de in deze verwerkersovereenkomst gemaakte afspraken aan te tonen. Indien Opdrachtgever desondanks aanleiding heeft aan te nemen dat de verwerking van Persoonsgegevens niet conform de verwerkersovereenkomst plaatsvindt, dan kan hij maximaal éénmaal per jaar door een onafhankelijke, gecertificeerde, externe deskundige die aantoonbaar ervaring heeft met het soort verwerkingen dat op basis van de Overeenkomst wordt uitgevoerd, op kosten van de Opdrachtgever hiernaar een audit laten uitvoeren. De audit zal beperkt zijn tot het controleren van de naleving van de afspraken met betrekking tot verwerking van de Persoonsgegevens zoals neergelegd in deze Verwerkersovereenkomst. De deskundige zal een geheimhoudingsplicht hebben ten aanzien van hetgeen hij aantreft en zal alleen datgene rapporteren aan Opdrachtgever dat een tekortkoming oplevert in de nakoming van verplichtingen die Data Processor heeft op grond van deze verwerkersovereenkomst. De deskundige zal een afschrift van zijn rapport aan Data Processor verstrekken. Data Processor kan een audit of instructie van de deskundige weigeren indien deze naar zijn mening in strijd is met de Avg of andere wetgeving of een ontoelaatbare inbreuk vormt op de door hem getroffen beveiligingsmaatregelen.

7.5 Partijen zullen zo snel mogelijk in overleg treden over de uitkomsten in het rapport. Partijen zullen de voorgestelde verbetermaatregelen die in het rapport zijn neergelegd opvolgen voor zover dat van hen in redelijkheid kan worden verwacht. Data Processor zal de voorgestelde verbetermaatregelen doorvoeren voor zover deze naar zijn oordeel passend zijn rekening houdend met de verwerkingsrisico’s verbonden aan zijn product of dienst, de stand van de techniek, de uitvoeringskosten, de markt waarin hij opereert, en het beoogd gebruik van het product of de dienst.

7.6 Data Processor heeft het recht om de kosten die hij maakt in het kader van het in dit artikel gestelde in rekening te brengen bij Opdrachtgever.

Artikel 8. Subverwerkers

8.1 Data Processor heeft in het Data Pro Statement vermeldt of, en zo ja welke derde partijen (subverwerkers) Data Processor inschakelt bij de verwerking van de Persoonsgegevens.

8.2 Opdrachtgever geeft toestemming aan Data Processor om andere subverwerkers in te schakelen ter uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst.

8.3 Data Processor zal Opdrachtgever informeren over een wijziging in de door de Data Processor ingeschakelde derde partijen bijvoorbeeld middels een aangepast Data Pro Statement. Opdrachtgever heeft het recht bezwaar te maken tegen voornoemde wijziging door Data Processor. Data Processor draagt ervoor zorg dat de door hem ingeschakelde derde partijen zich aan eenzelfde beveiligingsniveau committeren ten aanzien van de bescherming van de Persoonsgegevens als het beveiligingsniveau waaraan Data Processor jegens Opdrachtgever is gebonden op grond van het Data Pro Statement.

Artikel 9. Overig

Deze Standaardclausules voor verwerkingen vormen tezamen met het Data Pro Statement een integraal onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst, waaronder begrepen de van toepassing zijnde algemene voorwaarden en/of beperkingen van aansprakelijkheid, zijn derhalve ook van toepassing op de verwerkersovereenkomst.