DATA PRO STATEMENT

versie 2023-11A

Algemene informatie

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

   Korèn Information Technology B.V.

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

   Joeri Noort
   Managing Partner
   E-mail: joeri.noort@koren.nl
   Telefoonnummer: 030 - 231 61 32

2. **Dit Data Pro Statement geldt vanaf 25 mei 2018**
   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[1] 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**
   - KorènCRM
   - Korenter

   In alle gevallen waarbij in de onderstaande teksten KorènCRM wordt genoemd, wordt ook Korenter bedoeld.

4. **Omschrijving KorènCRM**
   KorènCRM is een SAAS oplossing voor ledenadministraties, verenigingen, non-profits, stichtingen, cursusaanbieders en zorgorganisaties op het gebied van relatiebeheer, ledenadministratie, cursusadministratie, alarmering, zorgbemiddeling en dienstverlening. Omdat er ook zorg (gerelateerde) gegevens in de software verwerkt kunnen worden is de software geschikt gemaakt voor het verwerken van bijzondere gegevens. Het aantal data subjects[2] is ongeveer 500.000.

   De dienst is doorgaans essentieel voor de klant om hun dagelijkse taken te kunnen verrichten. Een beperkt aantal medewerkers van Korèn kunnen in principe bij alle gegevens van klanten t.b.v. onderhoud en support. Zij zullen, tenzij anders afgesproken,

[1] partij die als ICT-leverancier in het kader van de uitvoering van de Overeenkomst als verwerker Persoonsgegevens verwerkt ten behoeve van diens Opdrachtgever.
[2] een geïdentificeerde of identificeerbare natuurlijke persoon.

geen persoonsgegevens[3] wijzigen of toevoegen, maar slechts inzien om een technisch probleem op te lossen.

5. **Beoogd gebruik**

KorènCRM is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:

Bij dit product is **wel** rekening gehouden met de verwerking van bijzondere persoonsgegevens namelijk medische gegevens. Zie de maatregelen privacy by design (punt 6 uit dit Data Pro Statement).

Deze software is **niet** bedoeld om de volgende bijzondere gegevens mee te verwerken: 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[4] 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 Korèn en zijn er mogelijk extra kosten verbonden hieraan.

Verwerken van deze gegevens met het hiervoor omschreven product of dienst door opdrachtgever[5] is ter eigen beoordeling door opdrachtgever.

---

[3] 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.

[4] de Algemene verordening gegevensbescherming.

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

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 i.v.m. 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 maar 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. Het is mogelijk om andere afspraken te maken echter zijn hier wel kosten aan verbonden.**

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 KorènCRM (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 in hun statement hebben aangegeven zich aan de regelgeving van de EU te houden.

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:**
    Voor KorènCRM heeft Korèn Information Technology BV 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 gebruikt gemaakt wordt van het systeem Te Veel Papier is Mailcamp b.v. ook een sub-verwerker. De sub-verwerkers van Mailcamp i.v.m. 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 t.b.v. support en onderhoud van KorènCRM gebruikers (medewerkers van de Verwerkingsverantwoordelijke) maakt data processor gebruik van Gsuite (Google LLC) als sub-verwerker.
    Voor contact als het gaat om projecten maakt data processor incidenteel gebruik van

Trello (Atlassian PTY Ltd).. Voor het verwerken van financiële gegevens t.b.v. de boekhouding is Reeleezee B.V. sub-processor.

12. **Data processor ondersteunt klanten op de volgende manier bij verzoeken van betrokkenen:**
    In KorènCRM is het mogelijk om zelf gegevens van data subjects / betrokkenen (in bulk) te verwijderen als een verzoek hiertoe binnenkomt. Daarnaast is het mogelijk om gebruik te maken van een gratis webapp waarmee betrokkenen hun NAW-gegevens, factuurhistorie, service- en Cursus aanvragen (indien er gebruik gemaakt wordt van deze modules) kunnen ontsluiten. NAW-gegevens kunnen hierin gewijzigd worden als ook contactgegevens zoals een e-mailadres en telefoonnummer.

    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 KorènCRM 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 kosten verbonden.

13. **Na beëindiging van de overeenkomst[6] 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 Korèn, 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 Korèn 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 verzoek

[6] 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.

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
KorènCRM wordt uitsluitend gehost vanuit datacentra op private dedicated servers die zich in Nederland bevinden en welke uitsluitend via de eerder genoemde beveiligde procedures te benaderen zijn. Korèn Information Technology BV heeft gekozen voor de datacentra van TransIP en deze is hiermee subbewerker 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 KorènCRM 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 Korèn geïsoleerd. De database waar de gegevens in worden opgeslagen is niet direct via internet toegankelijk en kan alleen via de KorènCRM 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. Korèn kan niet voorkomen dat door het gebruik van een geïnfecteerd systeem, gegevens worden blootgesteld aan derden, of dat bestanden welke in KorènCRM worden opgeslagen, het virus bij zich dragen. Korèn draagt er zorg voor dat eventuele virussen afkomstig uit het netwerk van de gebruiker, niet kunnen propageren binnen de instantie van KorènCRM, of tussen verschillende instanties van KorènCRM.

Monitoring
Data Processor geeft de applicatiebeheerder(s) de mogelijkheid om via gebruikersanalysetools verdachte of vreemde gebruikersactiviteit te monitoren en eventueel de noodzakelijke actie te ondernemen. Korèn stuurt maandelijks een rapport naar de applicatiebeheerder met een gebruiker statusoverzicht. Hierin staat o.a. wanneer een gebruiker voor het laatst heeft ingelogd en het aantal keer dat een gebruiker niet correct heeft uitgelogd. Korèn monitort ongewone server- of netwerkactiviteit via realtime monitoring tools. Data Processor neemt na het vaststellen hiervan indien noodzakelijk actie. In het geval dat de server onbereikbaar is zullen medewerkers van Data Processor hier binnen twee minuten automatisch van op de hoogte zijn. Hierdoor kan er indien noodzakelijk direct actie worden ondernomen.

Medewerkers van Korèn
Alle medewerkers van Korèn 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 Korèn 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. De Korèn helpdesk kan assisteren bij het gebruik hiervan.

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 Korèn 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 Korèn 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)[7] van het datalek.

Een datalek zal per e-mail met het onderwerp: “datalek melding” worden gemeld bij de contactpersoon van de Klant:

Contactgegevens van contactpersoon 1 van Verwerkingsverantwoordelijke:

Naam:

E-mailadres:

Telefoonnummer:

Contactgegevens van contactpersoon 2 van Verwerkingsverantwoordelijke:

Naam:

E-mailadres:

Telefoonnummer:

Inhoud van de melding:

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

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

Contactpersonen Korèn

De contactpersoon vanuit Korèn is Joeri Noort, bereikbaar per mail: joeri.noort@koren.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.