Data verwerkingsovereenkomst

Rekinéa VZW

Verwerkersovereenkomst NAAM PARTNER

Datum DATUM

Contractspartijen:

1. Verantwoordelijke te weten **Rekinéa VZW**, statutair gevestigd te **Agoralaan z/n te Diepenbeek**, vertegenwoordigd door IEMAND RAAD VAN BESTUUR

   Hierna te noemen: "**Ik**",

en

2. Verwerker te weten NAAM PARTNER, statutair gevestigd te ADRES PARTNER, vertegenwoordigd door CONTACTPERSOON

   Hierna te noemen: "**Jij**",

   Gezamenlijk aan te duiden als: "**Wij**";

Overwegend dat:

Wij hebben een overeenkomst gesloten met betrekking tot het doorgeven van e-mailadressen van studenten die wij verzameld hebben aan de hand van een inschrijfformulier. Ter uitvoering van onze overeenkomst worden er persoonsgegevens verwerkt.

Ik hecht grote waarde aan het beschermen van deze persoonsgegevens, daarom ben Ik verantwoordelijk voor de gegevens die Jij gaat verwerken en leggen Wij in deze verwerkersovereenkomst en de daarbij behorende bijlagen een:

1. Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen
2. Overzicht met beveiligingsmaatregelen
3. Proces rondom het melden van datalekken en de te verstrekken informatie

Vast wat Jij wel en niet mag doen met de Persoonsgegevens.

1. Definities

De hierna en hiervoor gebruikte begrippen volgen uit de Algemene Verordening Gegevensbescherming en hebben de volgende betekenis:

1-1 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon

1-2 Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via
geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

1-3 Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen ("Verantwoordelijke");

1-4 Verwerker: een natuurlijke persoon of rechtspersson, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt ("**Verwerker**");

1-5 Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte persoonsgegevens betrekking hebben;

1-6 Verwerkersovereenkomst: de ze overeenkomst inclusief de bijlagen ("**Verwerkersovereenkomst**");

1-7 Overeenkomst: de hoofdovereenkomst waar deze Verwerkersovereenkomst uit voortvloeit;

1-8 Inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens ("Datalek");

1-9 Gegevensbeschermingseffectbeoordeling: het uitvoeren van een beoordeling, voorafgaand aan het uitvoeren van de verwerking, van het effect van de beoogde verwerkingsactiviteiten op de bescherming van de persoonsgegevens.

1-10 Toezichthoudende autoriteit: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens;

2. Totstandkoming, duur en beëindiging van deze verwerkersovereenkomst

2-1 Deze Verwerkersovereenkomst treedt in werking op de datum waarop Wij deze ondertekenen.

2-2 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst en zal gelden voor zolang de Overeenkomst duurt.

2-3 Indien de Overeenkomst eindigt, eindigt deze Verwerkersovereenkomst automatisch; de Verwerkersovereenkomst kan niet apart worden opgezegd.

2-4 Na beëindiging van deze Verwerkersovereenkomst zullen de lopende verplichtingen voor jou, zoals het melden van Datalekken, waarbij de Persoonsgegevens van mij betrokken zijn, en de plicht tot geheimhouding blijven voortduren.

3. Verwerken persoonsgegevens

3-1 Jij zult alleen Persoonsgegevens verwerken in mijn opdracht en hebt geen zeggenschap over de Persoonsgegevens. Jij volgt mijn instructies hierover op en je mag de Persoonsgegevens niet op een andere manier verwerken, tenzij Ik jou daar van te voren toestemming of opdracht voor geef.

3-2 In Bijlage 1 wordt opgenomen welke Persoonsgegevens Jij precies zal verwerken en voor welke verwerkingsdoeleinden.

3-3 Jij houdt je aan de wet en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze.

3-4 Jij mag zonder mijn voorafgaande schriftelijke toestemming geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.

3-5 Wanneer Jij met mijn toestemming andere organisaties inschakelt, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Verwerkersovereenkomst.

3-6 Wanneer Ik een verzoek krijg van een Betrokkene die zijn of haar privacy rechten wil uitoefenen, werk je daar binnen een termijn van 14 dagen aan mee. Deze rechten bestaan uit een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van de persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens.

3-7 Wanneer Ik jou verzoek om mij informatie te geven, dan zal Jij de informatie verstrekken die ik nodig heb voor het uitvoeren van een Gegevensbeschermingseffectbeoordeling. Ik heb dit nodig om in te kunnen schatten wat het risico van de Verwerking is die Jij namens mij uitvoert.

10. Beveiligen van persoonsgegevens

4-1 Jij zorgt ervoor dat je de Persoonsgegevens voldoende beveiligt. Om verlies en onrechtmatige verwerkingen te voorkomen neem Jij passende technische en organisatorische maatregelen.

4-2 Deze maatregelen zijn afgestemd op het risico van de verwerking.

4-3 Ik mag een inspectie of audit in jouw organisatie laten uitvoeren om te bepalen of het verwerken van de Persoonsgegevens aan de wet en de afspraken uit deze Verwerkersovereenkomst voldoet. Hierbij zul Jij je medewerking verlenen, waaronder het toegang verlenen tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.

4-4 Wanneer een van ons vindt dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden Wij in overleg over de wijziging daarvan. De kosten voor het wijzigen van de beveiligingsmaatregelen komen voor de rekening van degene die de kosten maakt.

11. Exporteren persoonsgegevens

5-1 Jij mag geen Persoonsgegeven laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER), zonder daarvoor voorafgaande schriftelijke toestemming te hebben verkregen van mij.

12. Geheimhouding

6-1 Jij zult de aan jouw verstrekte Persoonsgegevens
geheim houden, tenzij dit op basis van een wettelijke verplichting niet mogelijk is.

6-2 Jij zult ervoor zorgen dat ook jouw personeel en ingeschakelde hulppersonen zich aan deze geheimhouding houden.

7. Datalekken

7-1 In geval van een ontdekking van een mogelijk Datalek zul Jij mij hierover informeren binnen 24 uur via praeses@rekinea.com en mij de informatie verstrekken die is aangegeven in Bijlage 2, zodat Ik indien nodig een melding bij de Toezichthouder kan doen.

7-2 Na de melding van een Datalek aan mij, zul je mij op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek en de maatregelen die Jij hebt getroffen om de omvang van het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen.

7-3 Het niet toegestaan dat Jij een melding van een Datalek doet aan de Toezichthouder en ook mag Jij de Betrokkenen niet informeren over het Datalek. Dit is mijn verantwoordelijkheid.

7-4 Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van degene die de kosten maakt.

8. Aansprakelijkheid

8-1 Als Jij jouw verplichtingen uit deze Verwerkersovereenkomst niet nakomt, stel Ik jou daarvoor aansprakelijk.

8-2 Jij bent aansprakelijk voor alle schade geleden door het niet nakomen van de wet en de bepalingen uit deze Verwerkersovereenkomst, voor zover dit is ontstaan door jouw werkzaamheden.

8-3 Ik ben niet aansprakelijk voor aanspraken van Betrokkenen of andere personen en organisaties waar Jij de samenwerking mee bent aangegaan of waarvan Jij Persoonsgegevens verwerkt, als dit het gevolg is van jouw onrechtmatig of nalatig handelen.

9. Teruggave Persoonsgegevens en bewaartermijn

9-1 Na het beëindigen van deze Verwerkersovereenkomst vernietig Jij deze persoonsgegevens.

9-2 De Persoonsgegevens die Jij verwerkt volgens deze Verwerkersovereenkomst zul je vernietigen na verstrijken van de wettelijke bewaartermijn en/of op verzoek van mij. Een wettelijke bewaartermijn is er bijvoorbeeld wanneer Jij de Persoonsgegevens moet bewaren om belastingtechnische redenen.

10. Slotbepaling

10-1 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op de Verwerkersovereenkomst.

10-2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de Verwerkersovereenkomst en de Overeenkomst, gelden de bepalingen uit deze Verwerkersovereenkomst.

10-3 Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig wanneer Wij dit samen schriftelijk afspreken.

10-4 Op deze Verwerkersovereenkomst en jouw werkzaamheden is het Belgische recht van toepassing.

10-5 Over eventuele geschillen tussen ons bepaald de rechter in de rechtbank binnen het gebied waar mijn bedrijf gevestigd is.

Aldus door ons overeengekomen en ondertekend:

Verantwoordelijke:

Ondertekend voor en namens:

Naam:

Functie:

Datum en plaats:

Handtekening

Verwerker:

Ondertekend voor en namens:

Naam:

Functie:

Datum en plaats:

Handtekening

Bijlage 1: Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen

Het onderstaande schema zal ingevuld moeten worden elke keer dat een Verwerkersovereenkomst wordt gesloten. Het geeft een volledig overzicht van de persoonsgegevens die verwerkt zullen worden. Dit maakt het makkelijker om aan te kunnen tonen waar, door wie en voor welk doel de persoonsgegevens worden verwerkt.

Beschrijving verwerkingsactiviteiten door Verwerker:

Verwerkingsdoelen:

Verwerkingsverantwoordelijke:

Verwerker:

Sub verwerkers:

Verwerkte Persoonsgegevens:

Locatie verwerkingen:

Bewaartermijn:

Bijlage 2: Proces rondom het melden van Datalekken en de te verstrekken informatie

Wat is een beveiligingsincident en wanneer moet dit gemeld worden?

Een datalek is een beveiligingsincident waarbij Persoonsgegevens, die de Verwerker namens de Verwerkingsverantwoordelijke beheert, mogelijk verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. Het gaat om gegevens die te koppelen zijn aan deze personen, zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, e-mailadressen, log in gegevens, cookies, IP adressen of identificerende gegevens van computers of telefoons.

Hieronder vind je een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens.

- De website met logingegevens is gehackt of is toegankelijk voor derden.
- Verlies van een laptop of USB-stick met persoonsgegevens.
- Salarisstroken van medewerkers zijn per ongeluk naar verkeerde personen gestuurd.
- Brieven of e-mails worden naar een verkeerd adres gestuurd.
- Een aanval van een hacker op het ICT systeem.
- Een verloren of gestolen telefoon waar persoonsgegevens op aanwezig

zijn. Wat te doen bij twijfel?

Als je op basis van bovenstaande niet zeker weet of er sprake is van een beveiligingsincident, stel je jezelf in ieder geval alvast de volgende vragen als hulpmiddel:

- Is er een technisch of fysiek beveiligingsprobleem?
- Gaat het probleem over de beveiliging van Persoonsgegevens? Ook IP-adressen, telefoonnummers of identificerende gegevens, bijvoorbeeld van hardware, kunnen hieronder vallen.
- Gaat het om gevoelige gegevens zoals ras, gezondheidsgegevens, informatie over iemands financiële situatie, zoals salaris of gegevens waar (identiteits)fraude mee kan worden gepleegd, zoals een Burgerservicenummer.
- Zijn er grote hoeveelheden persoonsgegevens onbedoeld toegankelijk geworden voor derden?
- Gaat het om gegevens van kwetsbare groepen zoals kinderen?
- Worden de persoonsgegevens beheerd door een leverancier?

Ook wanneer je twijfelt, neem het zekere voor het onzekere en neem altijd contact op met de praeses van Rekinéa via praeses@rekinea.com

Waar meld je het beveiligingsincident?

Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met de praeses van Rekinéa via het mailadres: praeses@rekinea.com.
Wij willen graag dat je de onderstaande vragen voor ons beantwoord. Deze vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt. (zie volgende bladzijde)

1. *Geef een samenvatting van het beveiligingslek / beveiligingsincident / datalek: wat is er gebeurd?*

Vermeld hier ook de naam van het betrokken systeem.

2. *Welke typen persoonsgegevens zijn betrokken bij het beveiligingsincident?*
   Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.
3. *Van hoeveel personen zijn de persoonsgegevens betrokken bij het beveiligingsincident?*
   Geef a.u.b. een minimum en maximum aantal personen.
4. *Omschrijving groep personen om wiens gegevens het gaat.*
   Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van een kwetsbare groepen personen, zoals kinderen.
5. *Zijn de contactgegevens van de betrokken personen bekend?*
   Het kan zijn dat betrokkenen geïnformeerd moeten worden over het datalek, kunnen we deze personen in dat geval bereiken?
6. *Wat is de oorzaak (root cause) van het beveiligingsincident?*
   Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?
7. *Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?*
   Geef dit a.u.b. zo specifiek mogelijk aan.