VERWERKERSOVEREENKOMST FANIC

Deze verwerkingsovereenkomst is een toevoeging aan de Overeenkomst tussen Fanic, gevestigd te Krimpen aan den IJssel, hierna te noemen: ***"JIJ" OF "JOU(W)"***, en de tegenpartij hierna te noemen: ***"IK" OF "MIJ(N)"***. Gezamenlijk aan te duiden als: ***"WIJ" OF "ONS"***;

DEZE VERWERKERSOVEREENKOMST GAAT ER VANUIT DAT

Wij een Overeenkomst hebben voor het uitvoeren van ICT diensten. Voor de uitvoering van onze Overeenkomst worden Persoonsgegevens verwerkt.

Ik hecht grote waarde aan het beschermen van deze Persoonsgegevens. Ik ben verantwoordelijk voor de gegevens die Jij gaat verwerken. Wij leggen in deze Verwerkersovereenkomst en de daarbij behorende bijlagen en informatie vast wat Jij wel en niet mag doen met de Persoonsgegevens.

AANVULLENDE BIJLAGEN DIE BIJ DEZE OVEREENKOMST HOREN

- Proces rondom het melden van Datalekken (Bijlage 1)
- Privacy statement met overzicht met verwerkingen van persoonsgegevens, verwerkingsdoelen en bewaartermijnen, te vinden op: https://www.fanic.com/privacy/
- Overzicht met beveiligingsmaatregelen, te vinden op https://www.fanic.com/security/

1 Begin, duur en beëindiging van deze Verwerkersovereenkomst

1.1 Deze Verwerkersovereenkomst treedt in werking op de datum waarop Wij deze ondertekenen.
1.2 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst en zal gelden voor zolang de Overeenkomst duurt.
1.3 Indien de Overeenkomst eindigt, eindigt deze Verwerkersovereenkomst automatisch; de Verwerkersovereenkomst kan niet apart worden opgezegd.
melden van Datalekken, waarbij de Persoonsgegevens van mij betrokken zijn, en de plicht tot geheimhouding blijven voortduren.

2 Verwerken Persoonsgegevens

2.1 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.
2.2 Jij zal persoonlijke e-mail en/of bestanden van Mij niet bekijken of delen met derden, tenzij:
- Ik mijn verplichtingen zoals beschreven in artikel 4 van de algemene voorwaarden niet nakom of er een vermoeden is dat ik dat niet doe;
- dat redelijkerwijs vereist is voor het uitvoeren van en onderhouden van Jouw diensten.
2.3 Bij het aangaan onze Overeenkomst geef ik aan welke soort Persoonsgegevens Jij zal verwerken en welke categorieën van betrokkenen het betreft. Tenzij anders aangegeven ga Jij er vanuit dat de Persoonsgegevens geen bijzondere Persoonsgegevens zijn en de volgende categorieën betrokkenen betreffen: (potentiële) klanten, websitebezoekers, werknemers. Ik sta ervoor in dat de omschreven persoonsgegevens en categorieën betrokkenen volledig en correct zijn, en vrijwaar Jou voor enige gebreken en aanspraken die resulteren uit een incorrecte weergave door Mij.
2.4 Jij houdt je aan de wet en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze.
2.5 Jij mag andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.
2.6 Wanneer Jij andere organisaties inschakelt, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Verwerkersovereenkomst.
2.7 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.

2.8 Bij een dergelijk verzoek zal Ik zelf dat verzoek in behandeling nemen en is het niet nodig dat Jij op de hoogte bent hoe ik dat verwerk.
2.9 Jij mag een redelijke, op daadwerkelijke kosten gebaseerde vergoeding vragen voor het verwerken van het verzoek.
2.10 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 (DPIA). Ik heb dit nodig om in te kunnen schatten wat het risico van de Verwerking is die Jij namens mij uitvoert.
2.11 Ik blijf ten alle tijde conform de AVG verantwoordelijk voor de verwerking van de gegevens door Jou en de daartoe door Jou genomen maatregelen ter beveiliging van de gegevens. Ik beoordeel of ik Jouw producten en of diensten kan gebruiken voor persoonsgegevens, bijzondere persoonsgegevens, of gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten.

3 Beveiligen van Persoonsgegevens

3.1 Jij zorgt ervoor dat je de Persoonsgegevens voldoende beveiligt. Om verlies en onrechtmatige verwerkingen te voorkomen neem Jij passende technische en organisatorische maatregelen.
3.2 Deze maatregelen zijn afgestemd op het risico van de verwerking. Een overzicht van deze maatregelen en het beleid neem je op in het 'Overzicht met beveiligingsmaatregelen', te vinden op https://www.fanic.com/security/
3.3 Ik mag een inspectie of audit in jouw organisatie laten uitvoeren door een onafhankelijke, derde partij welke onder vertrouwelijkheid en in overeenstemming met veiligheidseisen kan bepalen of het verwerken van de Persoonsgegevens aan de wet en de afspraken uit deze Verwerkersovereenkomst voldoet. Hierbij zal Jij naar redelijkheid je medewerking verlenen, waaronder het toegang verlenen tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.
3.4 Een inspectie of audit mag eenmaal per jaar worden uitgevoerd of in geval van een substantiële inbreuk op het gebruik van Persoonsgegevens.
3.5 De kosten voor de uitvoering van deze audit of inspectie betaal Ik.
3.6 De controle op de algehele verwerking van Persoonsgegevens door jou kan, naast de audit mogelijkheid, ook gebeuren via zelfevaluatie. Jij zal hierbij aan Mij een rapport verstrekken waarin Jij aantoont dat je voldoet aan de wet en de afspraken uit deze Verwerkersovereenkomst. Deze rapportage dient te worden ondertekend door een directielid binnen de jouw organisatie.
3.7 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.

4 Exporteren Persoonsgegevens

4.1 Jij mag geen Persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER) met uitzondering van landen die op basis van Artikel 45 van verordening 2016/679 aangemerkt worden als land waar geen aanvullende toestemming voor nodig is, zonder daarvoor voorafgaande schriftelijke toestemming te hebben verkregen van mij.

5 Geheimhouding

5.1 Jij zult de aan jouw verstrekte Persoonsgegevens geheim houden, tenzij dit op basis van een wettelijke verplichting niet mogelijk is.
5.2 Jij zult ervoor zorgen dat ook jouw personeel en ingeschakelde hulppersonen zich aan deze geheimhouding houden, door een geheimhoudingsplicht in de (arbeids-) contracten op te nemen.

6 Datalekken

6.1 In geval van een ontdekking van een mogelijk Datalek zul Jij mij hierover informeren binnen 36 uur via telefoon, e-mail of instant messaging en mij de informatie verstrekken die is aangegeven in Bijlage 1, zodat Ik indien nodig een melding bij de Toezichthouder kan doen.
6.2 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.
6.3 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.
6.4 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.

7 Aansprakelijkheid

7.1 Wij zijn overeen gekomen dat aansprakelijkheid is vastgelegd in de Overeenkomst. Tenzij anders afgesproken staat dit omschreven in de Algemene Voorwaarden van Fanic.

8 Teruggave persoonsgegevens en bewaartermijn

8.1 Na het beëindigen van deze Verwerkersovereenkomst geef Jij de Persoonsgegevens terug. Eventuele achtergebleven Persoonsgegevens zal je op een zorgvuldige en veilige manier vernietigen.
8.2 De Persoonsgegevens die Jij verwerkt volgens deze Verwerkersovereenkomst zal 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.
8.3 De Persoonsgevens die Jij bewaard kunnen na verwijdering mogelijk nog toegankelijk zijn vanaf een back-up medium, daarom zullen de betreffende Persoonsgegevens door Jou maximaal 3 maanden na verwijdering worden aangehouden in een register met verwijderde gegevens zodat na herstel van back-up gegevens deze (opnieuw) verwijderd kunnen worden.
8.4 Jij zal na de teruggave en/of vernietiging van de Persoonsgegevens schriftelijk aan mij verklaren dat je de Persoonsgegevens niet langer hebt.

9 Slotbepalingen

9.1 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op de Verwerkersovereenkomst.
9.2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de Verwerkersovereenkomst en de Overeenkomst, gelden de bepalingen uit deze Verwerkersovereenkomst.
9.3 Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig wanneer Wij dit samen schriftelijk afspreken.
9.4 Op deze Verwerkersovereenkomst en jouw werkzaamheden is het Nederlandse recht van toepassing.
9.5 Over eventuele geschillen tussen ons bepaald de rechter van de rechtbank van Rotterdam.

10 Definities

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

10.1 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
10.2 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;
10.3 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”);

10.4 VERWERKER: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de 3 verwerkingsverantwoordelijke persoonsgegevens verwerkt (“Bewerker”);
10.5 BETROKKENE: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte persoonsgegeven betrekking hebben;
10.6 VERWERKERSOVEREENKOMST: deze overeenkomst inclusief de bijlagen (“Bewerkersovereenkomst”);
10.7 OVEREENKOMST: de hoofdovereenkomst waar deze Verwerkersovereenkomst uit voortvloeit;
10.8 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”);
10.9 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.
10.10 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.

BIJLAGE 1: PROCES RONDOM HET MELDEN VAN DATALEKKEN EN DE VERTSTREKKEN 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 een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de toezichthouder.

- Verlies van een laptop of USB-stick met persoonsgegevens.
- De website met logingegevens is gehackt of is toegankelijk voor derden.
- 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?

MELDING BIJ DATALEK

In geval van een datalek zal de volgende informatie worden verstrekt, welke ook aan de toezichthouder zullen worden gemeld:

1. Een samenvatting van het beveiligingslek / beveiligingsincident / datalek: wat is er gebeurd? Inclusief 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? 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. 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?
5. Wat is de oorzaak (root cause) van het beveiligingsincident? Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?
6. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden? Geef dit a.u.b. zo specifiek mogelijk aan.