Kotuur Verwerkersovereenkomst

Deze privacyverklaring is opgesteld op 23-11-2020 door Mario de Bruin | Kotuur

Artikel 1. Inleiding

1.1 In het kader van artikel 28, lid 3 van de Algemene Verordening Gegevensbescherming is het verplicht dat een opdrachtgever een verwerkersovereenkomst (zie art. 2.9) sluit met een opdrachtnemer, indien deze over persoonsgegevens, zoals bedoeld in de Avg, beschikt of kan beschikken. De voorwaarden in deze verwerkersovereenkomst zijn bedoeld om beide partijen aan deze vereisten te laten voldoen.

1.2 Deze verwerkersovereenkomst is van toepassing op elke overeenkomst (zie art. 2.6) tussen opdrachtnemer en Kotuur die hiernaar verwijst, tenzij dat nadrukkelijk schriftelijk anders is overeengekomen.

1.3 De in deze verwerkersovereenkomst omschreven beveiligingsmaatregelen kunnen van tijd tot tijd door Kotuur worden aangepast aan veranderende omstandigheden. Kotuur zal opdrachtgever van significante aanpassingen per mail en via onze website op de hoogte stellen.

1.4 Deze verwerkersovereenkomst is opgesteld door Kodision, gevestigd te Arnhem, ingeschreven bij de Kamer van Koophandel onder nummer 08079430.

1.5 Voor vragen over deze verwerkersovereenkomst kan contact opgenomen worden met de Security Officer van Kotuur e-mail: Support@kotuur.nl t.a.v. Security Officer, telefoon: 026-3653560.

1.6 Deze verwerkersovereenkomst is van kracht vanaf 23-11-2020 en vervangt voorgaande versies van deze overeenkomst.

Artikel 2. Begrippen en definities

Onderstaande begrippen hebben in deze verwerkersovereenkomst de volgende betekenis:

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

2.2 Avg: de Algemene verordening gegevensbescherming. Inhoudelijk indentiek aan de Europese GDPR (General Data Protection Regulation).

2.3 Betrokkene: vertegenwoordigers en eindgebruikers van de opdrachtgever, zoals werknemers, opdrachtnemers, medewerkers en klanten.

2.4 Opdrachtgever: partij in wiens opdracht verwerker persoonsgegevens verwerkt. De opdrachtgever kan zowel verwerkingsverantwoordelijke (“controller”) zijn als een andere verwerker.

2.5 Opdrachtnemer: Kotuur, de partij die de werkzaamheden uitvoert in opdracht van de opdrachtgever.

2.6 Overeenkomst: de tussen opdrachtgever en opdrachtnemer geldende schriftelijke afspraak, op basis waarvan de ICT-leverancier diensten en/of producten levert aan opdrachtgever.

2.7 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals omschreven in artikel 4, sub 1 Avg, die verwerker in het kader van de uitvoering van zijn verplichtingen voortvloeiende uit de overeenkomst verwerkt.
2.8 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens in het kader van de Avg, verwerkt.
2.9 Verwerkersovereenkomst: overeenkomst voor verwerkingen, als bedoeld in artikel 28, lid 3 Avg.
2.10 Verwerkersverantwoordelijke: 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.

Artikel 3. Toepasselijkheid

3.1 Opdrachtnemer is verwerker in het kader van de Avg indien opdrachtnemer van opdrachtgever de beschikking krijgt over persoonsgegevens zoals bedoeld in de Avg.
3.2 Opdrachtnemer kan de beschikking krijgen over persoonsgegevens en heeft daarmee verwerkersverplichtingen, indien er sprake is van dat:
3.2.1 Opdrachtgever de software van opdrachtnemer hosted of ‘as a service’ afneemt bij opdrachtnemer, waarbij opdrachtgever zelf de inrichting en aard van de gerealiseerde toepassingen bepaalt.
3.2.2 Opdrachtnemer, uitsluitend op zijn eigen verzoek, bij het verlenen van supportdiensten voor het oplossen van productieverstoringen van opdrachtgever expliciet toegang heeft gekregen tot persoonsgegevens.

Artikel 4. Verwerkers statement

4.1 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.
4.2 Verwerker heeft in het kader van de Avg 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.
4.3 Verwerker verwerkt de persoonsgegevens namens en in opdracht van opdrachtgever overeenkomstig de met verwerker overeengekomen instructies, die impliciet vastliggen in de door opdrachtgever bepaalde configuratie en inrichting van de software. De aard en het doel van de verwerking is daarbij de levering te zvan de hosted of ‘as a service’-diensten alsmede de daaraan gerelateerde supportdiensten. Verwerker beperkt zich daarbij tot:
4.3.1 Het encrypted opslaan van de door de opdrachtgever uitgevraagde gegevens.

4.3.2 Het tijdelijk encrypted bewaren van de resultaten van een uitvraag voor verdere verzending.
4.3.3 Het periodiek, op basis van de door de opdrachtgever gespecificeerde frequentie, verwijderen van de encrypted opgeslagen gegevens.
4.3.4 Het maken en eventueel restoren van back-ups van de encrypted opgeslagen gegevens.
4.3.5 Het analyseren van ter beschikking gestelde logging t.b.v. support.

4.4 Verwerker geeft uitvoering aan de Avg zoals neergelegd in deze verwerkersovereenkomst en de overeenkomst. Opdrachtgever is eindverantwoordelijk om op basis van deze informatie te beoordelen of:
4.4.1 Verwerker afdoende garanties biedt om aan de vereisten van de Avg te voldoen.
4.4.2 De bescherming van de rechten van betrokkenen voldoende zijn gewaarborgd.

4.5 Opdrachtgever staat er tegenover verwerker 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 persoonsgegevens niet onrechtmatig zijn en geen inbreuk maken op enig recht van een derde.
4.6 Kotuur is slechts verwerker voor de duur van het gebruiksrecht dat opdrachtgever heeft ten aanzien van de hosted of 'as a service' dienst.
4.7 De typen persoonsgegevens die worden verwerkt door de hosted of 'as a service', zijn:
4.7.1 De typen zoals beschreven in art. 4 Avg.
4.7.2 Andere persoonsgegevens die door opdrachtgever worden verzonden naar de SaaSdienst of worden verstrekt in het kader van geleverde supportdiensten.

4.8 Wanneer er sprake is bijzondere categorieën van persoonsgegevens dient opdrachtgever dit expliciet te melden bij de verwerker.

Artikel 5. Verwerking binnen EU/EER

5.1 Verwerker verwerkt de persoonsgegevens van zijn opdrachtgevers binnen de EU/EER.
5.2 De primaire Hosting-omgeving bevindt zich in Nederland. In geval van calamiteiten blijven de gegevens binnen de EU/EER.

Artikel 6. Subverwerkers

6.1 Verwerker maakt gebruik van de volgende sub-processors:

- Microsoft, Evert van de Beekstraat 354, 1118 CZ Schiphol
- Previder, Expolaan 50, 7556 BE Hengelo
- Solvinity, Hogehilweg 3, 1101 CA Amsterdam

6.2 Opdrachtgever geeft, met inachtname van art. 6.3 en 6.4, toestemming aan verwerker om andere subverwerkers in te schakelen ter uitvoering van zijn verplichtingen voortvloeiende uit de overeenkomst.
6.3 Verwerker zal opdrachtgever informeren over een wijziging in de door de verwerker ingeschakelde derde partijen bijvoorbeeld middels een aangepaste verwerkersovereenkomst. Opdrachtgever heeft het recht bezwaar te maken tegen voornoemde wijziging door verwerker.
6.4 Verwerker draagt ervoor zorg dat de door hem ingeschakelde derde partijen zich aan 4 eenzelfde beveiligingsniveau committeren ten aanzien van de bescherming van de persoonsgegevens als het beveiligingsniveau waaraan verwerker jegens opdrachtgever is gebonden op grond van deze verwerkersovereenkomst.

Artikel 7. Beveiligingsmaatregelen

7.1 Kotuur heeft een Security Officer die verantwoordelijk is voor een adequaat informatiebeveiligingsbeleid en de daaruit voorvloeiende maatregelen waaronder het stimuleren van beveiligingsbewustzijn.
7.2 Een uitgebreide set van specifieke maatregelen op basis van het Internal Control framework (zie art 8) waaronder:

- Persoonsgegevens zijn geëncrypt en daarmee niet toegankelijk voor derden.
- Logische toegangscontrole, gebruik makend van sterke wachtwoorden.
- Beveiliging van netwerkverbindingen via Secure Socket Layer of vergelijkbare technologie. Zowel de hosting-, saasomgeving als de geleverde standaardsoftware ondergaan periodiek een pentest en worden geaudit en gecertificeerd.

7.3 Bij het treffen van de technische en organisatorische beveiligingsmaatregelen heeft verwerker 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 betrokkenes die hij gezien het beoogd gebruik van zijn producten en diensten mocht verwachten.
7.4 Het product of de dienst van verwerker is standaard niet ingericht op de verwerking van bijzondere categorieën van persoonsgegevens of gegevens betreffende strafrechtelijke veroordelingen of strafbare feiten. Tenzij dit schriftelijk overeengekomen is, of op basis van art. 4.8.
7.5 Verwerker streeft ernaar dat de door hem te treffen beveiligingsmaatregelen passend zijn voor het door verwerker beoogde gebruik van het product of de dienst.
7.6 De omschreven beveiligingsmaatregelen bieden, naar het oordeel van de opdrachtgever, rekening houdend met de in deze verwerkersovereenkomst genoemde factoren, een op het risico van de verwerking van de door hem gebruikte of verstrekte persoonsgegevens afgestemd beveiligingsniveau.

7.7 Verwerker kan wijzigingen aanbrengen in de getroffen beveiligingsmaatregelen indien dat naar zijn oordeel noodzakelijk is om een passend beveiligingsniveau te blijven bieden. Verwerker zal belangrijke wijzigingen vastleggen, bijvoorbeeld in een aangepaste verwerkersovereenkomst, en zal opdrachtgever waar relevant van die wijzigingen op de hoogte stellen.

7.8 Opdrachtgever kan verwerker verzoeken nadere beveiligingsmaatregelen te treffen. Verwerker is niet verplicht om op een dergelijk verzoek wijzigingen door te voeren in zijn beveiligingsmaatregelen. Verwerker kan de kosten verband houdende met de op verzoek van 5 opdrachtgever doorgevoerde wijzigingen in rekening brengen bij opdrachtgever. Pas nadat de door opdrachtgever gewenste gewijzigde beveiligingsmaatregelen schriftelijk zijn overeengekomen en ondertekend door partijen, heeft verwerker de verplichting deze beveiligingsmaatregelen daadwerkelijk te implementeren.

Artikel 8. Information Security Management System (ISMS)

Verwerker heeft zich geconformeerd aan een Internal Control Framework (ICF) dat is samengesteld is op basis van de volgende normen:

- ISO 27001: 2013 met aanvulling voor:
    - BIG
    - NCSC voor DigiD
    - TSP (Azure)

Minimaal jaarlijks wordt op basis van de ICF een audit uitgevoerd.

Artikel 9. Certificeringen

Verwerker heeft de volgende certificeringen:

- TPM DigiD Azure gebaseerd op Azure Public & Government SOC 2 Type 2
- ISAE3000 (Q2/2018) voor het onder 12 genoemde Internal Control Framework

Artikel 10. Inbreuken in verband met persoonsgegevens

10.1 Verwerker staat er niet voor in dat de beveiligingsmaatregelen onder alle omstandigheden doeltreffend zijn. Indien verwerker een inbreuk in verband met persoonsgegevens (zoals bedoeld in artikel 4 sub 12 Avg) ontdekt, zal hij opdrachtgever zonder onredelijke vertraging informeren. In het datalekprotocol (art. 11) is vastgelegd op welke wijze verwerker opdrachtgever informeert over inbreuken in verband met persoonsgegevens.

10.2 Het is aan de verwerkingsverantwoordelijke (opdrachtgever, of diens klant) om te beoordelen of de inbreuk in verband met persoonsgegevens waarover verwerker heeft

geïnformeerd gemeld moet worden aan de AP of betrokkene. 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 betrokkenes, blijft te allen tijde de verantwoordelijkheid van de verwerkingsverantwoordelijke (opdrachtgever of diens klant). Verwerker is niet verplicht tot het melden van inbreuken in verband met persoonsgegevens aan de AP en/of de betrokkene.

10.3 Verwerker 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.

10.4 Verwerker kan de redelijke kosten die hij in dit kader maakt in rekening brengen bij opdrachtgever tegen zijn dan geldende tarieven.

Artikel 11: Protocol bij datalekken

Verwerker hanteert in voorkomende gevallen het volgende datalekprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten:

- Een medewerker die een datalek vermoedt of constateert, meldt dit direct aan de Privacy Officer.
- De Privacy Officer registreert de melding en stelt vast of er daadwerkelijk sprake is van een datalek.
- De Privacy Officer stelt in het geval van een datalek de contactpersoon van de verwerkingsverantwoordelijke zonder onredelijke vertraging binnen 8 uur schriftelijk en telefonisch op de hoogte.
- De verwerkingsverantwoordelijke beoordeelt of het datalek moet worden gemeld aan de Autoriteit persoonsgegevens en is verantwoordelijk voor deze melding.
- De Privacy Officer verstrekt ingeval van een datalek alle relevante informatie over:
    - De kenmerken van het incident zoals: datum en tijdstip constatering, indicatie wanneer de inbreuk heeft plaatsgevonden, aard van de inbreuk, aard van de persoonsgegevens cq categorieën van betrokkeneen, schatting van aantal mogelijk geraakte datasubjecten en mogelijke gevolgen;
    - De maatregelen die zijn/worden genomen om de schade te beperken dan wel in de toekomst te voorkomen.
- De Privacy Officer sluit de melding als de maatregelen zijn afgerond en de verwerkingsverantwoordelijke akkoord is.

Artikel 12. Geheimhouding

12.1 Verwerker waarborgt dat de personen die onder zijn verantwoordelijkheid persoonsgegevens verwerken een geheimhoudingsplicht hebben.

12.2 Verwerker 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.

12.3 Alle door verwerker aan opdrachtgever verstrekte toegangs- en/of identificatiecodes, certificaten, informatie omtrent toegangs- en/of wachtwoordenbeleid en alle door Verwerker aan opdrachtgever verstrekte informatie die invulling geeft aan de in deze verwerkersovereenkomst 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 13. Rechten betrokkenen, Data Protection Impact Assessment (DPIA) en auditrechten

13.1 Verwerker zal, waar mogelijk, zijn medewerking verlenen aan redelijke verzoeken van 7 opdrachtgever die verband houden met bij opdrachtgever door betrokkenen ingeroepen rechten van betrokkenen. Indien verwerker direct door een betrokkene wordt benaderd, zal hij deze waar mogelijk doorverwijzen naar opdrachtgever.

13.2 Indien opdrachtgever daartoe verplicht is, zal verwerker 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.

13.3 Verwerker kan de naleving van zijn verplichtingen op grond van de verwerkersovereenkomst aantonen door middel van een geldig auditrapport (Third Party Memorandum) van een onafhankelijke deskundige, of daaraan ten minste gelijkwaardig certificaat.

13.4 Verwerker 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 verwerker heeft op grond van deze verwerkersovereenkomst. De deskundige zal een afschrift van zijn

rapport aan verwerker verstrekken. Verwerker 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.

13.5 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. Verwerker 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.

Artikel 14. Aansprakelijkheid, boetes, kosten

14.1 Kotuur is conform Avg, art 82, lid 2 Avg, als verwerker slechts aansprakelijk voor de schade die door verwerking is veroorzaakt wanneer bij de verwerking aantoonbaar niet is voldaan aan de specifiek tot verwerkers gerichte verplichtingen van de Avg of buiten dan wel in strijd met de rechtmatige instructies van de verwerkingsverantwoordelijke is gehandeld. Kotuur wijst 8 nadrukkelijk andere, niet in de Avg wettelijk vastgestelde aansprakelijkheden voor een verwerker, van de hand.

14.2 Kotuur vrijwaart opdrachtgever, op grond van de Avg, art 82, lid 2, nimmer op voorhand voor aansprakelijkheden door derden zoals eindgebruikers/cliënten.

14.3 Kotuur begrenst de maximale aansprakelijkheid tot hetgeen in de opdrachtovereenkomst en de geldende Algemene Voorwaarden is overeengekomen.

14.4 Een aan opdrachtgever door de AP opgelegde bestuurlijke boete kan uitsluitend o.b.v. wettelijke aansprakelijkheden zoals gedefinieerd in art. 14.1 worden verhaald op verwerker, tenzij er sprake is van opzet of bewuste roekeloosheid aan de zijde van de bedrijfsleiding van verwerker.

14.5 Kotuur begrenst de aansprakelijkheid tot de taken en verantwoordelijkheden, zoals die in de verwerkersovereenkomst is afgesproken.

14.6 Verwerker zal eventuele kosten die hij maakt op grond van werkzaamheden op verzoek van opdrachtgever, zoals bijvoorbeeld rapportages en audits, welke in het kader van de Avg niet als zodanig verplicht zijn, of in de gewenste frequentie niet wettelijk vereist zijn, in rekening brengen bij opdrachtgever.

Artikel 15. Looptijd en beëindiging

15.1 Deze verwerkersovereenkomst:

15.1.1 treedt in werking op het moment van totstandkoming van de overeenkomst (zie art 1.2 en 2.6) en wordt gesloten voor onbepaalde tijd;

15.1.2 eindigt van rechtswege bij beëindiging van de overeenkomst (zie art 1.2 en 2.6).

15.2 Verwerker zal, in geval van einde van de verwerkersovereenkomst, alle onder zich zijnde en van opdrachtgever ontvangen persoonsgegevens binnen de overeengekomen termijn verwijderen op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessable), of, indien overeengekomen, in een machine leesbaar formaat terugbezorgen aan opdrachtgever.

15.3 Het bepaalde in artikel 15.2 geldt niet indien een wettelijke regeling het geheel of gedeeltelijk verwijderen of terugbezorgen van de persoonsgegevens door verwerker belet. In een dergelijk geval zal verwerker de persoonsgegevens enkel blijven verwerken voor zover noodzakelijk uit hoofde van zijn wettelijke verplichtingen.