STANDAARD VERWERKERS-OVEREENKOMST

Bestaande uit:

Deel 1. Data Pro Statement

Deel 2. Standaardclausules voor verwerkingen

Versie januari 2018

DEEL 1: DATA PRO STATEMENT

Dit Data Pro Statement vormt samen met de Standaardclausules voor verwerkingen de verwerkersovereenkomst 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:**

   Make Life Easier B.V., Jaap Bijzerweg 19, 3446 CR Woerden
   Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met:
   Drs J.C. Wildenbeest RA, tel nr 030 3200 653, e-mail: johan@mle365.nl

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 data protectie steeds voorbereid en actueel te blijven. Wij houden u op de hoogte van nieuwe versies via onze normale kanalen.

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

   MLE 365 samenstel en/ of MLE 365 controle.

4. **Omschrijving MLE 365 samenstel en MLE 365 controle**
   MLE 365 samenstel: Software-as-a-Service (SaaS) voor het geïntegreerd opbouwen van een jaarrekening, een samensteldossier en een SBR instance. MLE 365 samenstel wordt gehost in Microsoft Azure.
   MLE 365 controle: Software-as-a-Service (SaaS) voor het risicogericht uitvoeren van jaarrekening controles. MLE 365 controle wordt gehost in Microsoft Azure.
   Meer informatie over de software is te vinden op de website: www.mle365.nl

5. **Beoogd gebruik**
   MLE 365 samenstel en/ of MLE 365 controle is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:
   MLE 365 samenstel
   Gegevens welke nodig zijn voor het opstellen van een jaarrekening, een SBR instance en een samensteldossier conform de geldende wet- en regelgeving waaronder onder andere: SBR/ XBRL, COS 4410, Titel 9 BW 2, RJ, Leidraden NBA,
   MLE 365 controle
   Gegevens welke nodig zijn voor het controleren van een jaarrekening inclusief de daar bijbehorende dossiervorming conform de geldende wet- en regelgeving waaronder onder andere de NV COS.

6. **Bij dit product/deze dienst is niet rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten mee te verwerken. Verwerken van deze gegevens met het hiervoor omschreven product of dienst door opdrachtgever is ter eigen beoordeling door opdrachtgever.**

7. **Data processor heeft bij het ontwerpen van het product/de dienst *privacy by design* op de volgende wijze toegepast:**
   Gegevens die nodig zijn voor uitvoeren van accountantsopdrachten worden uitgevraagd. Klanten vullen zelf hun gegevens in, inclusief door hen gekozen bijlagen en kunnen deze gegevens en documenten wijzigen en verwijderen. Data processor controleert de gegevens niet en zal gegevens alleen inzien op verzoek van klant, bijvoorbeeld als dat nodig is om een vraag aan de helpdesk te beantwoorden.

8. **Data processor gebruikt de Data Pro Standaardclausules voor verwerkingen, welke als deel 2: standaarclausules voor verwerkingen zijn opgenomen.**

9. **Data processor verwerkt de persoonsgegevens van zijn opdrachtgevers binnen de EU/EER.**

10. **Data processor maakt gebruik van de volgende sub-processors:**
    Goed om te weten: Microsoft is verwerker voor MLE 365. Als u werkt met MLE 365 samenstel en/ of MLE 365 controle dan staat de data in een Microsoft Azure datacenter. MLE 365 zorgt ervoor dat de data binnen de Europese economische zone blijft, zodat uw data altijd onder de Europese wet- en regelgeving verwerkt wordt en beschermd is. Wilt u meer weten over de verwerkingsafspraken tussen Make Life Easier B.V. en Microsoft, lees dan de serviceovereenkomsten van Microsoft.

11. **Na beëindiging van de overeenkomst met een opdrachtgever verstrekt de data processor de opgeslagen data binnen 3 maanden aan de opdrachtgever. Na de datum van verstrekking verwijdert data processor de data die hij voor opdrachtgever verwerkt in principe binnen 3 maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible).**

12. **Bewaartermijn data**
    Data processor bewaart de opgeslagen data conform de geldende wettelijke bewaartermijnen. Na het verstrijken van de wettelijke bewaartermijn verwijdert data processor de data die hij voor opdrachtgever verwerkt in principe binnen 3 maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible). Opdrachtgever kan voor het verstrijken van de wettelijke bewaartermijn een verzoek indienen om de data te verstrekken aan de opdrachtgever.

BEVEILIGINGSBELEID

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

De samenvatting van de getroffen beveiligingsmaatregelen is opgenomen in de Bijlage beveiligingsmaatregelen.

14. Data processor heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):

- ISO 27001

15. Data processor heeft de volgende certificeringen

Data processor host bij Microsoft Azure en deze beschikken o.a. over de volgende certificeringen:

- Microsoft Azure beschikt over ISO 27001 certificering: https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec-27001
- Voor Microsoft Azure en ISAE 3402 zie : https://azure.microsoft.com/en-us/blog/security-privacy-compliance-update-availability-of-ssae-16-isae-3402-attestation/

DATALEKPROTOCOL

16. 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:

Meldplicht datalekken

De AVG vereist dat eventuele datalekken gemeld worden aan de Autoriteit Persoonsgegevens door de verwerkingsverantwoordelijke van de data. Data processor zal daarom zelf geen meldingen doen bij de Autoriteit Persoonsgegevens. Uiteraard zal Data processor als verwerker de klant juist, tijdig en volledig informeren over relevante incidenten, zodat de klant als verwerkingsverantwoordelijke aan zijn wettelijke verplichtingen kan voldoen. De Beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens geven hierover meer informatie.

Bepaling datalek

Voor het bepalen van een datalek, gebruikt Data processor de AVG en de Beleidsregels meldplicht datalekken als leidraad. Onder een datalek vallen alle beveiligingsincidenten waardoor de bescherming van persoonsgegevens op enig moment is doorbroken of waardoor de persoonsgegevens blootgesteld zijn aan verlies of onrechtmatige verwerking. Het kan bijvoorbeeld gaan om het verlies van een USB-stick of computer, inbraak door een hacker, verzending van een e-mail waarin de e-mailadressen zichtbaar zijn voor alle geadresseerden, een malwarebesmetting of een calamiteit zoals brand in een datacenter.

Indien de klant een (voorlopige) melding verricht bij de Autoriteit Persoonsgegevens en/of de betrokkene(n) over een datalek bij Data processor, terwijl zonder meer voor de klant duidelijk is dat bij Data processor geen sprake is van een datalek dan is de klant aansprakelijk voor alle door Data

processor geleden schade en kosten. De klant is daarnaast verplicht een dergelijke melding direct in te trekken.

Melding aan de klant

Indien blijkt dat bij Data processor sprake is van een datalek, dat door de klant gemeld moet worden aan de Autoriteit Persoonsgegevens en/of de betrokkene(n), dan zal Data processor de klant daarover zo spoedig mogelijk informeren nadat Data processor bekend is geworden met het datalek. Om dit te realiseren zorgt Data processor ervoor dat al haar medewerkers in staat zijn en blijven om een datalek te constateren en verwacht Data processor van haar opdrachtnemers dat zij Data processor in staat stelt om hier aan te kunnen voldoen. Voor de duidelijkheid: als er een datalek is bij een leverancier van Data processor, dan meldt Data processor dit uiteraard ook.Data processor is het contactpunt voor de klant. De klant hoeft geen contact op te nemen met de leveranciers van Data processor.

Informeren klant
In eerste instantie zal Data processor de contactpersoon van het abonnement informeren over een datalek.

Informatie verstrekken
Data processor probeert de klant direct alle informatie te verstrekken die de klant nodig heeft om een volledige melding bij de Autoriteit Persoonsgegevens en/of de betrokkene(n) te verrichten. Indien deze informatie nog niet bekend is, bijvoorbeeld omdat het datalek door Data processor wordt onderzocht, dan zal Data processor de klant de informatie verstrekken die de klant nodig heeft om in ieder geval eerst een voorlopige melding bij de Autoriteit Persoonsgegevens en/of de betrokkene(n) te kunnen verrichten. Hierbij volgt Data processor de informatielijst uit de eerdergenoemde beleidsregels. Dit bevat in ieder geval de aard van de inbreuk, een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk en de getroffen en te treffen maatregelen om de negatieve gevolgen van het datalek te beperken en te verhelpen.

Termijn van informeren
De AVG geeft aan dat er ‘onverwijld’ gemeld moet worden. Dit is volgens de Autoriteit Persoonsgegevens zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na ontdekking. Data processor informeert de klant daarom zo snel mogelijk, uiterlijk binnen 48 uur na het ontdekken van een datalek, zodat de klant tijdig de melding kan doen bij de Autoriteit Persoonsgegevens.

Voortgang en maatregelen
Data processor zal de klant op de hoogte houden over de voortgang en de maatregelen die getroffen worden. Data processor maakt hierover afspraken met de primaire contactpersoon bij de initiële melding. In ieder geval houdt Data processor de klant op de hoogte in geval van een wijziging van de situatie, het bekend worden van nadere informatie en over de maatregelen die getroffen worden.

Juist, tijdig en volledig
Data processor registreert alle security incidenten en handelt deze volgens een vaste procedure (workflow) af. De registratie en afhandeling van security incidenten wordt getoetst met een audit.

DEEL 2: STANDAARDCLAUSULES VOOR VERWERKINGEN

versie: januari 2018

Vormt samen met het Data Pro Statement de verwerkersovereenkomst en is een bijlage bij de Overeenkomst en de daarbij behorende bijlagen zoals toepasselijke algemene voorwaarden

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.

1.3 **Data Processor**: 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 inaccessable*), 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 een geldig Data Pro Certificaat of daaraan ten minste gelijkwaardig certificaat of auditrapport (Third Party Memorandum) van een onafhankelijke, deskundige.

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.

BIJLAGE SAMENVATTING BEVEILINGSMAATREGELEN

MLE 365 applicaties draaien op het Azure-platform van Microsoft (Datacenter West Europe), dat voldoet aan de hoogste veiligheidseisen. Zie voor beveiligingsmaatregelen die zijn getroffen: http://www.microsoft.com/download/en/details.aspx?id=26647

In aanvulling daarop neemt Make Life Easier B.V. (MLE) technische en organisatorische maatregelen binnen MLE ter bescherming van persoonsgegevens tegen verlies of onrechtmatige verwerking. Een samenvatting van de maatregelen is hieronder opgenomen.

TOEGANGSCONTROLE EN INTERGRITEITSCONTROLE

MLE heeft de volgende maatregelen getroffen om te borgen dat geautoriseerde gebruikers van een gegevensverwerkingssysteem alleen toegang hebben tot de gegevens waarvoor ze zijn bevoegd en de integriteit van gegevensverwerkingssystemen te bewaken:

- Role & Access management
- Authenticatie door middel van gebruiksnaam en wachtwoord
- Monitoring en locatiebeperking van het gebruik van administrator accounts
- Two Factor Authenticatie voor administrator portal
- Minimumeisen aan samenstelling wachtwoorden
- Gebruik van disk encryptie op servers, laptops en andere gegevensdragers
- Procedure voor tijdig updaten systemen
- Gebruik van een beveiligde Gateway
- Systemen maken gebruik van anti-virus software
- Systemen maken gebruik van thread-detection-Software
- Actieve monitoring logfiles op security issues
- Gebruik van Web-Applicatie-Firewall (WAF)
- Vulnerability scans en penetratie testen
- Medewerkers hebben een geheimhoudingsovereenkomst ondertekend
- Medewerkers kunnen uitsluitend na autorisatie door gebruiker meekijken

BESCHIKBAARHEID

De volgende maatregelen zijn geïmplementeerd om ervoor te zorgen dat persoonsgegevens worden beschermd tegen onopzettelijke vernietiging of verlies:

- Monitoring beschikbaarheid servers en netwerkverkeer
- Back-up en recovery procedures: minimaal 2 keer per dag backup van system images en data
- Periodieke test van terugzetten van back-up
- Beveiligde opslag van offsite back-ups (datacenter North Europe)

GESCHEIDEN VERWERKING

De volgende maatregelen zijn geïmplementeerd om ervoor te zorgen dat gegevens die voor verschillende opdrachtgevers worden verwerkt, afzonderlijk kunnen worden verwerkt:

- Databank autorisatiematrix
- Procedure voor uitgeven databankrechten
- Logische (softwarematige) scheiding van gegevens van klanten
- Productiesysteem gescheiden van ontwikkel- test- en acceptatiesysteem

TOEZICHT OP INVOER VAN GEGEVENS

De volgende maatregelen zijn geïmplementeerd worden om ervoor te zorgen dat het mogelijk is om te bepalen en te controleren of en door wie persoonlijke gegevens zijn ingevoerd, gewijzigd of verwijderd op gegevensverwerkingssystemen:

- Gebruiksrechten toevoegen, wijzigen en verwijderen van data zijn gebaseerd op de autorisatiematrix
- Registratie van invoeren, wijzigingen en verwijderen van data
- Herleidbaarheid van invoer, wijzigingen en verwijderen van data tot een individuele gebruiker
- Periodiek controleren van toegekende bevoegdheden.