Versie: 1.5 / 28 maart 2024

Verwerkers-overeenkomst FuseLogic BV

Bestaande uit:

Deel 1. Data Pro Statement

Deel 2. Standaardclausules voor verwerkingen

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 de volgende data processor (verwerker):**
   FuseLogic BV, gevestigd te Olympia 2d, 1213 NT, Hilversum

   Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met:
   - Leon Oud (leon.oud@fuselogic.nl, 06-13352305) en
   - Bert Dondertman (bert.dondertman@fuselogic.nl, 06-55716255)

2. **Dit Data Pro Statement geldt vanaf 28 maart 2024 (v1.5)**
   Dit Data Pro Statement en de daarin 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**

Dienst
a. 3e lijn support Okta (Dienst)
b. Okta Connectoren (Product)

4. **Omschrijving Product/Dienst**

   a De dienst 3e lijn support Okta omvat:
   - 3e lijn support issues en incidenten worden door opdrachtgever gemeld via het support portal.
   - FuseLogic registreert het ticket na ontvangst en wijst het toe aan een support-medewerker;
   - FuseLogic reageert na ontvangst met een eerste inschatting van de oplossingsrichting, de oplostijd en planning, dan wel verzoek voor nadere informatie of overleg.
   - FuseLogic probeert het issue of incident op te lossen of er wordt een vervolg gepland;

   b Okta Connectoren omvat:
   - Hosten van een connector tussen een Okta tenant en AFAS/TopDesk tenant

   N.B. Connector bevat geen persisterende klantdata. Enkel ‘on the fly’ tussen de systemen stroomt er klantdata door de connector.

5. **Beoogd gebruik**

a Dienst 3e lijn Okta Support is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken: Naam en emailadres van de klantcontactpersonen

Bij dit product/deze dienst is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers. Verwerken van deze gegevens met het hiervoor omschreven dienst door opdrachtgever is ter eigen beoordeling door opdrachtgever.

b Product Okta Connectoren is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken: NAW, Email, Telefoonnummer, Functie, Rol en Afdeling

Bij dit product/deze dienst is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers. Verwerken van deze gegevens met het hiervoor omschreven product door opdrachtgever is ter eigen beoordeling door opdrachtgever.

6. **Data processor heeft bij het ontwerpen van het product/de dienst privacy by design/privacy by default op de volgende wijze toegepast:**

a Dienst 3e lijn Okta Support : de opdrachtgever draagt verantwoordelijkheid voor de in de melding aanwezige gegevens, inclusief door opdrachtgever gekozen bijlagen. Opdrachtgever kan 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. Onze helpdesk webformulieren bevatten alleen verplichte velden die nodig zijn om het incident te melden. Alle andere velden kunnen optioneel gebruikt worden op verzoek van de opdrachtgever.

b Product Okta Connectoren : Transport Level Security (TLS 1.2) , geen opslag van gegevens in de connector (incl log files of tijdelijke bestanden), Multi Factor Toegang tot administratie consoles.

7. **Data processor gebruikt de Standaardclausules voor verwerkingen, welke als bijlage bij de Overeenkomst te vinden zijn.**

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

9. **Data processor maakt gebruik van de volgende sub-processors:**

a Dienst 3e lijn Okta Support:

- Microsoft Office365 met gebruik van een EU-datacenter.
- Atlassian Jira Service Desk met gebruik van een EU-datacenter.
- Atlassian Confluence met gebruik van een EU-datacenter.
- AFAS – ERP met gebruik van een EU datacentre
- Slack team communicatie (https://slack.com/trust/compliance/gdpr)
- Hubspot CRM / Marketing campaigns (https://www.hubspot.com/data-privacy/gdpr)

- 1Password - password management (https://support.1password.com/1password-privacy/)

b Product Okta Connectoren :

- Amazon Web Services met gebruik van een EU datacentre

10. **Data processor ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:**
    - Inzage-, correctie- en verwijder- en dataportabiliteitsverzoeken worden vergemakkelijkt door:
    - Selectiemogelijkheden voor de opdrachtgever om zelf te zoeken naar tickets, meldingen en deze, indien gewenst en mogelijk, aan te passen.
    - Gebruik te maken van de toegang tot de rapportage mogelijkheden over tickets en meldingen.
    - Op aanvraag is inzage, correctie en verwijdering van persoonsgegevens mogelijk

11. **Verwijdering na beëindiging van de overeenkomst**
    Na beëindiging van de Overeenkomst met een opdrachtgever verwijdert data processor de persoonsgegevens 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).

Beveiligingsbeleid

12. **Data processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:**
    zie Bijlage Beveiligingsmaatregelen FuseLogic BV, gebaseerd op checklist NLDigital.

13. **Data processor heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):**
    - ISMS NL Digital

14. **Data processor heeft de volgende certificeringen:**
    - Data Pro Certificate

Datalekprotocol

15. **In geval er toch iets mis gaat, hanteert data processor het volgende datalekprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten:**
    Indien de data processor in zijn organisatie een datalek ontdekt, zal de data processor zijn opdrachtgever daarvan zo snel mogelijk op de hoogte stellen:

    - door telefonisch contact op te nemen met de contactpersonen van opdrachtgever zoals beschreven in het support contract.
    - door een email te sturen aan de contactpersonen van opdrachtgever zoals beschreven in het support contract..

Data processor levert zo veel mogelijk relevante gegevens aan, waaronder omschrijving van het incident, aard van de inbreuk, aard persoonsgegevens c.q. categorieën van betrokken data subjects, schatting van aantal betrokken data subjects en mogelijk betrokken databases, indicatie wanneer incident heeft plaatsgevonden (wat is er gebeurd); Contactgegevens contactpersoon (waar kan de opdrachtgever met vragen terecht); Mogelijke gevolgen (wat kan er gebeuren, waar moet opdrachtgever dan wel data subject op bedacht zijn, wijzen op mogelijkheden identiteitsfraude als gegevens als BSN nummers, inlog en wachtwoordgegevens, paspoort kopieën etc. in verkeerde handen terecht zijn gekomen); Genomen maatregelen (wat heeft de data processor gedaan om eventuele schade te beperken of dit in de toekomst te voorkomen); Te nemen maatregelen door de opdrachtgever dan wel betrokken data subjects (wat kunnen betrokken data subjects zelf doen, bijvoorbeeld “houd mail in de gaten, wijzig passwords”);

Meldingen worden indien mogelijk binnen 24 uur gedaan aan opdrachtgever. Data processor zal zelf geen meldingen doen aan AP of data subjects. Wel of niet melden blijft de verantwoordelijkheid van de opdrachtgever. De data processor zal de opdrachtgever desgewenst ondersteunen bij het meldproces.

Data processor levert zo veel mogelijk relevante gegevens aan, waaronder omschrijving van het incident, aard van de inbreuk, aard persoonsgegevens c.q. categorieën van betrokken data subjects, schatting van aantal betrokken data subjects en mogelijk betrokken

Deel 2: Standaardclausules voor verwerkingen

Versie: september 2019

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, sub-processors, 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.

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 of door de overheid uitgegeven persoonsnummers.

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 aan 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 zal zijn medewerking verlenen aan verzoeken van Opdrachtgever tot het verwijderen van persoonsgegevens voor zover Opdrachtgever dit niet zelf kan uitvoeren.

7.4 Data Processor kan desgewenst de naleving van zijn verplichtingen op grond van de verwerkersovereenkomst aantonen door middel van een geldig Data Pro Certificaat of een daaraan ten minste gelijkwaardig certificaat of auditrapport (Third Party Memorandum) van een onafhankelijke, deskundige, indien hij over een dergelijk certificaat of auditrapport beschikt.

7.5 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.

7.6 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.

7.7 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. Sub-Processors

8.1 Data Processor heeft in het Data Pro Statement vermeld of, en zo ja welke derde partijen (sub-processors of subverwerkers) Data Processor inschakelt bij de verwerking van de Persoonsgegevens.

8.2 Opdrachtgever geeft toestemming aan Data Processor om andere sub-processors 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.

Heb je vragen?

Onze juristen kunnen je voorzien van advies en ondersteuning. Neem contact met ons op.

NLdigital organiseert ook verschillende juridische workshops en bijeenkomsten. Houd hiervoor de agenda op onze website in de gaten. Leden van NLdigital kunnen hier kosteloos aan deelnemen. Ben je nog geen lid en wil je ook profiteren van deze en vele andere mogelijkheden van het lidmaatschap? Bekijk de voordelen!

NLdigital
De Corridor 5
3621 ZA Breukelen
info@nldigital.nl
+31 (0) 348 - 49 36 36
KVK 3017 4840

NLdigital

CHECKLIST BEVEILIGINGS-MAATREGELEN

Versie: maart 2024

INLEIDING: ALGEMENE PRINCIPES IN DE AVG OVER BEVEILIGING

Een van de beginselen uit de Avg is dat persoonsgegevens door het nemen van passende technische en organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging ('integriteit en vertrouwelijkheid').

Andere principes zijn dat er niet meer gegevens verwerkt mogen worden dan nodig (dataminimalisatie), dat maatregelen genomen moeten worden om te zorgen dat persoonsgegevens actueel zijn (juistheid), dat ze niet langer bewaard worden dan nodig ('opslagbeperking') of dat principes als 'privacy by design' en 'privacy by default' worden toegepast.

In de Data Pro Code wordt nadere invulling gegeven aan deze beveiligingsbeginselen en worden best practices aangegeven.

Organisaties die in opdracht van een andere partij persoonsgegevens verwerken, de 'verwerkers' (in het Engels 'data processors'), hebben met name te maken met het beginsel van beveiliging. De opdrachtgever, meestal de 'verwerkingsverantwoordelijke' (of in het Engels 'controller'), mag op grond van de Avg alleen in zee gaan met data processors die aantoonbaar hun beveiligingsmaatregelen op orde hebben.

Er staan geen concrete beveiligingsmaatregelen in de Avg. De wet zegt dat er rekening moet worden gehouden met de stand van de techniek, de uitvoeringskosten van de beveiligingsmaatregelen, de aard van de persoonsgegevens, de omvang, context en verwerkingsdoeleinden en de te verwachten risico's. De te kiezen technische en organisatorische maatregelen dienen op dat risico te zijn afgestemd, zodat uiteindelijk een passend beveiligingsniveau wordt gewaarborgd.

Partijen die met persoonsgegevens werken moeten zelf een belangenafweging maken waarbij de genoemde factoren worden meegewogen. Klanten die hun verwerkingen bij een data processor laten uitvoeren zijn verplicht zich ervan te gewissen dat de beveiliging bij de data processor passend is. Een data processor die de Data Pro Code volgt, moet zijn opdrachtgevers informeren over de keuze van zijn beveiligingsmaatregelen en waarom die passend zijn bij zijn product of dienst.

Die keuzes worden door de data processor opgenomen in zijn Data Pro Statement. Bij het implementeren van de Data Pro Code en door het invullen van het Data Pro Statement worden data processors ondersteund om zelf die keuzes van passende beveiligingsmaatregelen te maken.

Als extra handreiking is onderstaand een uitgebreide checklist opgenomen met concrete beveiligingsmaatregelen die een partij zou kunnen nemen. Deze lijst is niet uitputtend. Afhankelijk van jouw product of dienst, de kosten en de daaraan verbonden risico's kun je je eigen keuzes maken om tot een passende beveiliging te komen. De lijst met mogelijke

beveiligingsmaatregelen dient ter inspiratie. Vanzelfsprekend kun je andere en nadere beveiligingsmaatregelen kiezen indien die voor jouw product en/of dienst beter passen.

TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

1. Fysieke toegangscontrole (gebouw / kantoor / datacenter)

Zijn binnen je organisatie maatregelen getroffen om de fysieke toegangsbeveiliging te waarborgen? Zo ja, welke? De volgende maatregelen kunnen onder andere genomen worden om ongeoorloofde toegang te voorkomen tot gegevensverwerkingssystemen waar persoonsgegevens worden verwerkt:

- ☒ Automatische toegangscontrole
- ☒ Veiligheidssloten (handmatig en/of elektronisch)
- ☒ Sleutelbeheer (sleutel uitgifte, etc.)
- ☒ Bezoekersregistratie
- ☐ Zichtbaar dragen van bezoekerspas
- ☒ Bewegingsmelders
- ☐ Screening personeel (waaronder ook beveiliging en schoonmaak)
- ☒ Camera toegangsbewaking
- ☒ Alarmsysteem
- ☒ Een gedocumenteerde toegangscontrole voor datacenters en serverruimten. Toegang alleen voor bevoegde personen, naam en kaart- of sleutelnummer wordt geregistreerd.

2. Toegangscontrole tot systemen (systemen / computers / servers / randapparatuur)

Heeft jouw organisatie maatregelen om te borgen dat enkel geautoriseerd personeel toegang heeft tot de gegevens in de IT-systemen? Zo ja, welke? De volgende maatregelen kunnen onder andere worden genomen om het gebruik van gegevensverwerkingssystemen door onbevoegde personen te voorkomen:

☒ Medewerkers hebben een geheimhoudingsverklaring ondertekend
☒ Medewerkers worden getraind op informatiebeveiligingsbewustzijn
☒ Medewerkers worden gescreend of hebben een VOG-verklaring
☒ Role & Access management (toewijzen van individuele gebruiksrechten (account met privileges))
☒ Toewijzen van individuele gebruiksnamen
☒ Toewijzen van individuele wachtwoorden
☐ Authenticatie door middel van gebruiksnaam en wachtwoord
☒ Two Factor Authenticatie door middel van gebruiksnaam en wachtwoord
☒ Minimumeisen aan samenstelling wachtwoorden
☒ Aparte gebruiksrechten voor ICT-systemen
☒ Gebruik van VPN-software
☐ Encryptie van mobiele datadragers (USB)
☐ Centraal beheer van smartphones (met mogelijke om remote data te wipen)
☒ Gebruik van disk encryptie bij laptops / notebooks
☒ Gebruik van softwarematige firewall (gebruikerssystemen)
☐ Implementatie van Intrusion-Prevention-Systeem
☒ Implementatie van Firewalls

3. Integriteitscontrole (systemen / computers / servers / randapparatuur)

Worden ICT veranderingen in de organisatie procesmatig uitgevoerd? Zo ja, op welke wijze?
Beschikt uw organisatie over maatregelen die de IT-omgeving beschermen tegen virussen en malware?
Wordt er periodiek een beveiligingsonderzoek op de IT-systemen in uw organisatie uitgevoerd?
De volgende maatregelen kunnen onder andere worden genomen om de integriteit van gegevensverwerkingssystemen te bewaken:

☒ Gedocumenteerde procedure voor updaten van systemen
☒ Wachtwoorden hebben minimale complexiteit
☐ Wachtwoorden worden periodiek gewijzigd
☒ Systemen maken gebruik van anti-virus software
☐ Systemen maken gebruik van Intrusion-Detection-Software (IDS)
☐ Gebruik van Web-Applicatie-Firewall (WAF)
☒ Periodieke vulnerability scan
☒ Periodieke penetratie testen
☐ Gedocumenteerde procedure voor responsible disclosure
☒ Logfiles worden periodiek bekeken
☒ Gedocumenteerde procedure voor melden beveiligingsincidenten

4. Toegangscontrole tot data

Hanteert de organisatie logging en monitoring van gebruikers- en beheerders-activiteiten in relatie tot de bewerking van de gegevens en wordt deze logging periodiek gecontroleerd? Dit voorkomt dat persoonlijke gegevens worden gelezen terwijl deze gegevens in gebruik zijn, onderweg, of opgeslagen zijn zonder dat daarvoor toestemming verkregen is. De volgende maatregelen kunnen onder andere worden genomen om ervoor te zorgen dat geautoriseerde gebruikers van een gegevensverwerkingssysteem alleen toegang hebben tot de gegevens waarvoor ze zijn bevoegd:

- ☒ Gebruik van een autorisatiematrix
- ☒ Procedure voor uitgeven van administrator / root rechten
- ☒ Procedure voor gebruik van administrator / root rechten
- ☒ Registratie van switchen naar adminstrator / root rechten
- ☒ Registratie van gebruik adminstrator / root rechten
- ☒ Registratie van toegang tot applicaties, speciaal bij invoeren, aanpassen of verwijderen van data
- ☒ Disk encryptie van back-up tapes bij off-site tape storage en laptops
- ☒ Wachtwoordpolicy met daarin beschreven: minimale lengte van het wachtwoord en verplichte periodieke wijziging
- ☒ Media worden veilig opgeslagen
- ☒ Veilig wissen van media voor hergebruik, afdanking
- ☒ Veilig vernietigen van media bij afdanking
- ☒ Registratie van uitgifte van media
- ☐ Registratie van wissen, vernietigen van media

5. Beveiliging van gegevens in transit

Hanteert de organisatie beveiligingsmaatregelen voor gegevens in transit, zoals versleuteling (encryptie) van gegevens? Zo ja, welke? De volgende maatregelen kunnen onder andere worden geïmplementeerd om ervoor te zorgen dat persoonsgegevens niet kunnen worden gelezen, gekopieerd of gewijzigd tijdens elektronische verzending of tijdens transport of opslag op schijf. Daarnaast om te controleren en te bepalen aan welke instanties de overdracht van persoonlijke gegevens door gegevenscommunicatieapparatuur is toegestaan:

- ☐ Gebruik van VPN tunnels bij gebruik van WiFi
- ☒ Disk encryptie (back-up tapes bij off-site opslag)
- ☒ TLS encryptie van alle communicatie (Web-Client, APIs, mobile Apps)

6. Toezicht op invoer van gegevens

Is je organisatie in staat om gegevens te anonimiseren dan wel te pseudonimiseren? De volgende maatregelen kunnen onder andere 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:

- ☒ Registratie van invoeren, wijzigingen en verwijderen van data
- ☒ Herleidbaarheid van invoer, wijzigingen en verwijderen van data tot een individuele gebruiker
- ☒ Gebruiksrechten toevoegen, wijzigen en verwijderen van data zijn gebaseerd op de autorisatiematrix
- ☒ Creëren van een overzicht van in welke applicaties het is toegestaan om welke gegevens in te voeren, te wijzigen of te verwijderen
- ☐ Opslag van formulieren, via welke gegevens zijn verkregen tijdens de geautomatiseerde verwerking
- ☐ Anonimiseren of pseudonimiseren van persoonsgegevens

7. Toezicht op subverwerkers

Maakt de organisatie voor de levering van diensten gebruik van hosting e/o SAAS diensten? Zo ja, welke en welke maatregelen zijn genomen om de beveiliging te borgen? De volgende maatregelen kunnen onder andere geïmplementeerd worden om ervoor te zorgen dat persoonsgegevens door subverwerkers alleen worden verwerkt zoals de opdrachtgever heeft opgedragen:

- ☒ Selectie van (sub)verwerker met inachtneming data security geschiedenis.
- ☒ (sub)verwerker heeft gedocumenteerde procedures m.b.t. de AVG.
- ☒ (sub)verwerker heeft functionaris voor de gegevensverwerking
- ☒ Effectieve controlemaatregelen zijn afgesproken met de (sub)verwerker
- ☒ Onderzoek naar documentatie en genomen beveiligingsmaatregelen door (sub)verwerker
- ☐ Werknemers bij (sub)verwerker hebben geheimhoudingsplicht
- ☒ Vernietiging van data na afloop contract is vastgelegd
- ☒ Periodieke evaluatie van door (sub)verwerker genomen maatregelen.
- ☒ Afspraken zijn vastgelegd in een (sub)verwerkersovereenkomst, bijvoorbeeld in een Data Pro Statement met bijbehorende Standaardclausules voor verwerking

8. Beschikbaarheid

Worden binnen de organisatie back-ups van de gegevens gemaakt en worden deze afdoende beveiligd en op een ander locatie opgeslagen? Voert de organisatie periodiek, als test, een restore van de back-up uit? Zo ja, hoe vaak? De volgende maatregelen kunnen onder andere

worden geïmplementeerd om ervoor te zorgen dat persoonsgegevens worden beschermd tegen onopzettelijke vernietiging of verlies:

- ☒ Stroomvoorziening gegarandeerd door Uninterruptible power supplies (UPS)
- ☒ Temperatuur en luchtvochtigheid wordt gemeten in server
- ☒ Brand- en rookmelders
- ☒ Alarmering op toegang serverruimte
- ☒ Periodieke test van terugzetten van back-up
- ☒ Beveiligde opslag van offsite back-ups
- ☒ Airconditioning of koeling in serverruimte
- ☒ Gezekerde stroomvoorziening
- ☒ Blusinstallatie in serverruimte
- ☒ Back-up en recovery procedures zijn gedocumenteerd
- ☒ Gedocumenteerd noodplan
- ☒ Uitwijklocatie

9. Gescheiden verwerking

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

- ☒ Databank autorisatiematrix
- ☒ Gegevensvelden in een database hebben een toegewezen doelattribuut
- ☒ Goedgekeurde en gedocumenteerde procedure voor uitgeven databankrechten
- ☒ Logische (softwarematige) scheiding van gegevens van klanten
- ☒ Gebruik van aparte OTAP-straat
- ☒ Productiesysteem gescheiden van ontwikkel- test- en acceptatiesysteem
- ☐ Bij gebruik pseudonieme data: toewijzingsbestand is opgeslagen op een afzonderlijke server