Verwerkersovereenkomst

VERSIE 8 BBE 01.04.2024

§ 1. Doel van de Verwerkersovereenkomst

(1) De Verwerker verleent diensten aan de Verwerkingsverantwoordelijke (hierna ook: “klant”) zoals geregeld in de onderliggende overeenkomst tot verhuur/aankoop van multifunctionele kopieerapparaten met bijhorende onderhoudsdiensten (hierna: de ‘Hoofdovereenkomst”). Voor zover de levering van deze diensten onder de hoofdovereenkomst de verwerking van persoonsgegevens namens de verantwoordelijke inhoudt, zoals bedoeld in de Algemene Verordening Gegevensbescherming die op 25 mei 2018 in werking is getreden (hierna: AVG), leggen de partijen hierbij hun respectieve rechten en verplichtingen vast in de onderhavige verwerkersovereenkomst

(2) Persoonsgegevens die onder de Verwerkersovereenkomst verwerkt worden, kunnen afkomstig zijn van de Verwerkingsverantwoordelijke of van verwerkers die verbonden zijn met de Verwerkingsverantwoordelijke in de zin van art. 26 of 28 van de AVG, of van gegevens verzameld door de Verwerker voor de voormelde partijen (al deze data worden hierna collectief ‘persoonsgegevens van de Verwerkingsverantwoordelijke’ genoemd).

(3) Het type persoonsgegevens van de Verwerkingsverantwoordelijke die door de Verwerker worden verwerkt, de verschillende categorieën van betrokkenen bij de verwerking en de aard en het doel van de verwerking worden verder gespecificeerd in bijlage 1 van deze verwerkersovereenkomst.

(4) De looptijd van deze verwerkersovereenkomst is in principe gelijk aan de duurtijd van de Hoofdovereenkomst, tenzij voor de verplichtingen of rechten uit deze overeenkomst die verder reiken dan de duurtijd van de Hoofdovereenkomst.

§ 2. Instructies van de verwerkingsverantwoordelijke

(1) De Verwerker mag alleen gegevens verzamelen, verwerken of gebruiken binnen het toepassingsgebied van de Hoofdovereenkomst en in overeenstemming met de instructies van de Verwerkingsverantwoordelijke.

(2) De instructies van de Verwerkingsverantwoordelijke worden in eerste instantie bepaald in deze Verwerkersovereenkomst en kunnen later gewijzigd, aangevuld of vervangen worden door afzonderlijke instructies op schrift of per e-mail (afzonderlijke instructies.) Mondelinge instructies worden direct, tenminste digitaal, bevestigd door de verwerkingsverantwoordelijke. De Verwerkingsverantwoordelijke is bevoegd op elk moment instructies door te geven. Hieronder vallen instructies betreffende wissen, rectificeren en beperken van dataverwerking.

Voor diensten waarvoor het geven van instructies is vereist, zijn in de **bijlagen** van deze overeenkomst personen aangewezen die instructies mogen geven en ontvangen.

(3) Als de Verwerker van mening is dat een instructie van de Verwerkingsverantwoordelijke in strijd is met regelgeving t.a.v. het beschermen van persoonsgegevens, moet de Verwerkingsverantwoordelijke zo snel mogelijk gewaarschuwd worden. De Verwerker is gemachtigd de uitvoering van de instructie in kwestie op te schorten tot deze is bevestigd of aangepast door de Verwerkingsverantwoordelijke. De Verwerker mag weigeren een instructie uit te voeren die onwettig is.

(4) Als de Verwerkingsverantwoordelijke instructies geeft die niet vallen onder de diensten als genoemd in de Hoofdovereenkomst en de daarvoor benodigde gegevensverwerking, dan kan de Verwerker deze instructies supplementair factureren aan de verwerkingsverantwoordelijke.

§ 3. Veiligheidsmaatregelen van de Verwerker

(1) De Verwerker is verplicht zich te houden aan de bepalingen van de AVG. De Verwerker zal zich zo organiseren dat zij voldoet aan de speciale vereisten betreffende gegevensbescherming als opgelegd door de AVG. De Verwerker zal alle benodigde technische en organisatorische maatregelen voor de juiste bescherming van de persoonsgegevens nemen conform art. 32 van de AVG, met name en tenminste de maatregelen opgesomd in de bijlage 1 bij deze overeenkomst. De Verwerker behoudt zich het recht voor de genomen veiligheidsmaatregelen aan te passen, waarbij hij ervoor zorgt dat ze niet minder bescherming bieden als de bescherming die is opgenomen in bijlage aan deze overeenkomst.

(2) De Verwerker heeft een functionaris voor gegevensbescherming aangesteld. De contactgegevens van de functionaris voor gegevensbescherming zijn op de website van de Verwerker gepubliceerd.

(3) De Verwerker zal een geheimhoudingsplicht (art. 28 (3) b AVG) opleggen aan haar personeel of aangestelden die belast zijn met de verwerking en het nakomen van deze overeenkomst (hierna te noemen 'medewerkers') en zal met de nodige zorgvuldigheid ervoor zorgen dat deze verplichting wordt nagekomen.

§ 4. Rechten van de Verwerker

(1) In het geval er een inbreuk in verband met persoonsgegevens van de Verwerkingsverantwoordelijke heeft plaatsgevonden, zal de Verwerker de verwerkingsverantwoordelijke onmiddellijk schriftelijk of per e-mail hiervan informeren. De melding van de inbreuk op persoonsgegevens moet ten minste het volgende beschrijven:

a. aard van de inbreuk op de persoonsgegevens, inclusief waar mogelijk de categorieën en bij benadering het aantal personen die het betreft, en de categorieën en bij benadering het aantal bestanden van de persoonsgegevens;

b. naam en contactgegevens van de functionaris gegevensbescherming of andere contactpersonen waar meer informatie verkregen kan worden;

c. waarschijnlijke gevolgen van de inbreuk op persoonsgegevens;

d. genomen of voorgestelde maatregelen uit te voeren door de Verwerkingsverantwoordelijke om de inbreuk op persoonsgegevens aan te pakken/te herstellen, inclusief, waar passend, te nemen maatregelen om mogelijke negatieve effecten in te perken.

(2) De Verwerker zal onmiddellijk de nodige maatregelen nemen om de persoonsgegevens te beveiligen en alle eventuele negatieve gevolgen voor de betreffende personen te beperken. Hij zal de verwerkingsverantwoordelijke hiervan op de hoogte stellen en nadere instructies vragen.

(3) Daarnaast is de Verwerker verplicht op elk moment de Verwerkingsverantwoordelijke informatie te verschaffen omtrent een inbreuk op persoonsgegevens zoals genoemd in artikel 4.1.

(4) Als de persoonsgegevens van de Verwerkingsverantwoordelijke bij de Verwerker gevaar lopen door beslaglegging of confiscatie, door insolventie- of arbitrageprocedures of door andere acties of maatregelen van derden, dan zal de Verwerker de Verwerkingsverantwoordelijke onmiddellijk hierover informeren, tenzij dit door de rechtbank of door een officieel bevel verboden is. In dat geval zal de Verwerker direct alle gerechtelijke autoriteiten informeren dat de uiteindelijke beslissingsbevoegdheid over de gegevens exclusief bij de Verwerkingsverantwoordelijke ligt in diens capaciteit als 'verantwoordelijke' zoals omschreven in de AVG.

(5) De Verwerker zal bijhouden welke verwerkingsactiviteiten hebben plaatsgevonden voor de Verwerkingsverantwoordelijke, waarbij hij er zorg voor draagt dat alle informatie zoals omschreven in art. 30 (2) van het AVG is opgenomen.

(6) De Verwerkingsverantwoordelijke en de Verwerker zullen, mochten zij daartoe verzocht worden, de toezichthoudende autoriteiten van gegevensbescherming assisteren in het uitoefenen van hun functies.

§ 5. Rechten van de Verwerkingsverantwoordelijke

(1) De Verwerkingsverantwoordelijke zal, alvorens met de verwerking gestart wordt en regelmatig daarna, bepalen of de technische en organisatorische maatregelen zoals genomen door de Verwerker voldoende adequaat zijn. Hiervoor kan de Verwerkingsverantwoordelijke, bijvoorbeeld, informatie vragen van de Verwerker, hij kan bestaande certificaten of getuigschriften van experts of, zij het aangekondigd binnen een redelijke termijn (minimaal drie weken van tevoren), de technische en organisatorische maatregelen van de Verwerker

inspecteren aan de hand van een audit. Audits kunnen persoonlijk of door een geschikte derde partij uitgevoerd worden tijdens normale kantooruren. Audits door een derde partij moeten uitgevoerd worden met instemming van de Verwerker, derden die een concurrentiepositie innemen met de Verwerker kunnen door hem afgewezen worden. De Verwerkingsverantwoordelijke zal alleen audits uitvoeren in zoverre dat noodzakelijk is en zal de normale bedrijfsactiviteiten van de Verwerker niet in onevenredige mate verstoren. Iedere partij zal zijn eigen kosten dragen met betrekking tot een inspectie of audit.

(2) De Verwerker verplicht zich de Verwerkingsverantwoordelijke, na diens schriftelijke verzoek en binnen een redelijke termijn, alle benodigde informatie te verschaffen benodigd voor een audit of inspectie van de technische en organisatorische maatregelen die de Verwerker getroffen heeft.

(3) De Verwerkingsverantwoordelijke zal het resultaat van de audit of inspectie delen met de Verwerker. Mocht de Verwerkingsverantwoordelijke fouten of onregelmatigheden ontdekken, vooral in de resultaten van in opdracht verwerkte persoonsgegevens, dan zal de Verwerker per omgaande geïnformeerd worden. Als de audit of inspectie zaken blootlegt die in de toekomst vermeden moeten worden en als dit wijzigingen in de verwerkersactiviteiten met zich zou meebrengen, dan zal de Verwerkingsverantwoordelijke de Verwerker van die bevindingen en de nodige veranderingen schriftelijk of per e-mail op de hoogte stellen.

§ 6. Inschakelen Subverwerkers

(1) Door ondertekening van deze overeenkomst, krijgt de Verwerker een algemene toestemming om Subverwerkers aan te stellen voor de uitvoering van de Hoofdovereenkomst. Een lijst van de aangestelde Subverwerkers is opgenomen in bijlage 1 van deze overeenkomst.

(2) De Verwerker is gerechtigd om bestaande Subverwerkers te vervangen of nieuwe Subverwerkers aan te stellen. De verwerker zal de verwerkingsverantwoordelijke hiervan zo snel als mogelijk informeren. De klant beschikt steeds over de mogelijkheid bezwaar te uiten tegen deze vervanging of wijziging wegens het niet respecteren van de AVG door deze Subverwerker. Dit bezwaar mag niet gebaseerd zijn op onredelijke motieven die los staan van de Hoofdovereenkomst tussen partijen en moet onmiddellijk na kennisname geschieden.

(3) De Verwerker is verplicht Subverwerkers zorgvuldig te selecteren gelet op hun geschiktheid en betrouwbaarheid. Als er gebruik wordt gemaakt van Subverwerkers, dan zal de Verwerker ze in dienst nemen in overeenstemming met de voorwaarden van deze Verwerkersovereenkomst. Als er Subverwerkers in een ander land worden gebruikt, zal de Verwerker ervoor zorgen dat er een behoorlijk niveau van databescherming gegarandeerd is voor de betreffende Subverwerkers(bijv. middels overeenstemming t.a.v. standaard Europese contractclausules).

(4) Er is geen sprake van de aanstelling van een Subverwerker in de zin van de AVG als de Verwerker derden de opdracht geeft tot de uitvoering van zuiver ondersteunende diensten. Daartoe behoren, bijvoorbeeld, post- , transport- en opslagdiensten, schoonmaakdiensten, diensten

betreffende telecommunicatie die niet speciifiek betrekking hebben op de diensten die de Verwerker voor de verwerkingsverantwoordelijke verricht, en beveiligingsdiensten.

§ 7. Vragen en rechten van betrokkenen

(1) Waar mogelijk zal de Verwerker de verwerkingsverantwoordelijke ondersteunen met de juiste technische en organisatorische maatregelen om diens verplichtingen t.a.v. art. 12 tot 22 en 32 van de AVG te helpen vervullen.

(2) Mocht een betrokkene contact opnemen van de Verwerker om hun recht als betrokkene te laten gelden, bijvoorbeeld om informatie te verkrijgen of om zijn persoonsgegevens te wijzigen of te wissen, dan zal de Verwerker deze vraag delen met de Verwerkingsverantwoordelijke. Als de Verwerkingsverantwoordelijke middels het verzoek van de betrokkene geïdentificeerd kan worden, zal de Verwerker de Verwerkingsverantwoordelijke op de hoogte stellen en diens instructies afwachten.

§ 8. Aansprakelijkheid

(1) De Verwerkingsverantwoordelijke aanvaardt binnen de grenzen van de hoofdovereenkomst de volledige verantwoordelijkheid voor enige vordering jegens de Verwerker wegens verlies of schade geleden door een betrokkene ten gevolge van een verwerking van persoonsgegevens die verboden of incorrect is op grond van de AVG en voor zover het verboden of incorrecte gebruik van persoonsgegevens is gebaseerd op instructies van de Verwerkingsverantwoordelijke.

(2) De verwerkingsverantwoordelijke of verwerker worden van aansprakelijkheid vrijgesteld indien zij bewijzen dat zij op geen enkele wijze verantwoordelijk zijn voor het schadeveroorzakende feit.

§ 9. Beëindiging van de Hoofdovereenkomst

(1) Na beëindiging van de Hoofdovereenkomst of wanneer de Verwerkingsverantwoordelijke daarom vraagt, zal de Verwerker aan de Verwerkingsverantwoordelijke alle documenten, gegevens en gegevensdragers die door de Verwerkingsverantwoordelijke zijn verstrekt hetzij teruggeven hetzij - als hij daarom verzoekt en behalve wanneer er een wettelijke verplichting bestaat de persoonsgegevens op te slaan – vernietigen of overschrijven. De verwerker is gerechtigd om de verwerkingsverantwoordelijke kosten aan te rekenen voor een vernietiging of overschrijving van de persoonsgegevens op de harde schijf van een multifunctioneel kopieerapparaat.

(2) De Verwerker is verplicht de gegevens vertrouwelijk te behandelen waarvan hij kennis heeft genomen met betrekking tot de Hoofdovereenkomst(en) gedurende en na afloop van de duur van de Hoofdovereenkomst(en). Deze verplichting blijft ook van kracht na afloop van de duur van

de Hoofdovereenkomst(en) zo lang de Verwerker nog de beschikking heeft over de persoonsgegevens van de Verwerkingsverantwoordelijke.

§ 10. Algemene bepalingen

(1) Wijzigingen en aanvullingen aan deze overeenkomst dienen schriftelijk te geschieden.

(2) Deze Verwerkersovereenkomst vormt een integraal onderdeel van de Hoofdovereenkomst. Alle rechten en verplichtingen uit de Hoofdovereenkomst, waaronder begrepen beperkingen van aansprakelijkheid, zijn derhalve ook van toepassing op deze Verwerkersovereenkomst. In geval van tegenstrijdigheid, dubbelzinnigheid of twijfel tussen de bepalingen van deze Verwerkersovereenkomst en de bepalingen van de Hoofdovereenkomst, heeft de Hoofdovereenkomst voorrang.

(3) Indien (een) afzonderlijke bepaling(en) van deze overeenkomst in zijn geheel of ten dele ongeldig of niet-afdwingbaar is of wordt verklaard zal dit geen invloed hebben op de geldigheid van de andere bepalingen uit deze overeenkomst.

(4) Deze overeenkomst wordt beheerst door Belgisch Recht en in geval van een geschil zal, naar keuze van Verwerker, de rechtbank van Brussel of Antwerpen bevoegd zijn.

Bijlage 1 tot de verwerkersovereenkomst

Beschrijving van de technische en organisatorische beveiligingsmaatregeling

1. A) Beschrijving van de aard en het doel van de verwerking bij Printsystemen

Konica Minolta Multifunctionele en/of Production Printingsystemen (“Konica Minolta systemen”) verwerken papieren en elektronische documenten voor het afdrukken, scannen, kopiëren en faxen.

De verwerking van persoonsgegevens van de Verwerkingsverantwoordelijke of derden (hierna gezamenlijk aangeduid als "Controller") door Konica Minolta vindt uitsluitend plaats in het kader van het verlenen van service en onderhoud op de Konica Minolta systemen. Bijkomende verzameling of gebruik van de persoonsgegevens van de Controller door Konica Minolta vindt niet plaats. De specifieke aard van de verwerking is afhankelijk van de in deze bijlage beschreven serviceopties en diensten op afstand waarvoor de Controller heeft gekozen.

De verwerking van persoonsgegevens van de Controller kan plaatsvinden bij het beschikbaar stellen en instellen van de Konica Minolta Systemen (met name in het kader van een netwerkverbinding) en bij fysieke onderhoudswerkzaamheden aan de Konica Minolta systemen.

Konica Minolta systemen kunnen technische processen vastleggen in geëncrypteerde logbestanden. Konica Minolta begint pas met het aanmaken van logbestanden wanneer een foutenanalyse van het Konica Minolta systeem noodzakelijk is. De logbestanden kunnen door een technicus van Konica Minolta ter plaatse worden geraadpleegd, maar in de standaardprocedure worden de logbestanden overgebracht naar servers die eigendom zijn van en beheerd worden door Konica Minolta Europe (serverlocatie Duitsland) als onderdeel van de Konica Minolta remote services (Konica Minolta "Remote Service Platform" - "RSP").

Bovendien kunnen reservekopieën van de configuratie (instellingen) worden gemaakt die in een met een wachtwoord beveiligde en geëncrypteerde vorm kunnen worden opgeslagen op de eigen servers van de Controller of op de servers van Konica Minolta Europe (serverlocatie Duitsland).

Zowel de logbestanden als de reservekopieën van de Konica Minolta systemen bevatten geen inhoud van afdrukken, scannen, kopiëren of soortgelijke bewerkingen die op de systemen zijn uitgevoerd.

Onderhoud op afstand van de Konica Minolta Systemen kan worden uitgevoerd. Hiervoor gebruikt Konica Minolta het "Konica Minolta Remote Service Platform" (RSP), Remote Panel verbindingen, de oplossing "Konica Minolta Remote Support Tool", of functioneel vergelijkbare oplossingen. Bij het uitvoeren van onderhoud op afstand is het niet uit te sluiten dat Verwerker inzage krijgt in persoonsgegevens van de Controller.

In het geval van een eventuele teruggave van Konica Minolta Systemen na afloop van de looptijd van de Hoofdovereenkomst, zullen de persoonsgegevens op de harde schijf en in het interne geheugen van de Konica Minolta systemen worden vernietigd, overschreven of teruggegeven worden aan de Controller.

1. B) Beschrijving van de aard en het doel van de verwerking bij Safe Q Cloud oplossingen

SafeQ Cloud is een alles-in-één cloudoplossing voor printbeheer en scannen, ontworpen voor organisaties die zichzelf willen ontzorgen bij het runnen van een complexe IT-printinfrastructuur en tegelijkertijd willen profiteren van alle voordelen van een Software-as-a-Service (SaaS)-aanbod. De software wordt beheerd en gehost door Konica Minolta Europe in datacentra in Duitsland en Zweden die eigendom zijn van Konica Minolta Europe.

Tijdens het aanbieden en uitvoeren van de Safe Q Cloud Dienst heeft Konica Minolta toegang tot de persoonlijke gegevens van de Controller en/of persoonlijke gegevens van andere derde partijen zoals bv. gegevens van gegevensbeheerders en betrokkenen.

Van belang is dat Konica Minolta de Persoonsgegevens van de Controller verwerkt voor en met als enig doel het verlenen van de Dienst. Er vindt geen verzameling, gebruik of verwerking van de Persoonsgegevens van de Controller plaats die de bovengenoemde doeleinden overschrijdt.

2.1. A) Aard van de persoonsgegevens bij Printsystemen

Algemeen: gegevens van Betrokkenen waartoe Konica Minolta in het kader van de Hoofdovereenkomst met de klant toegang tot krijgt.

Persoonsgegevens die kunnen zijn opgenomen in back-up kopies: het adresboek van het kopieerapparaat (IT gebruikersnamen en e-mailadressen van gebruikers), IP adressen, MAC adressen, serienummer

Persoonsgegevens die mogelijk zijn opgenomen in logbestanden:
IT-gebruikersnamen (bijvoorbeeld Windows-gebruikersnamen van de gebruikers van het apparaat), e-mailadressen van gebruikers, IP-adressen, MAC-adressen, serienummer, geschiedenis van de internetbrowser van het apparaat (bezochte URL's), geschiedenis van de stroomstatus van het apparaat, geschiedenis van de laatste 150 printopdrachten (eigenaar van de printopdracht, tijdstempel, documentnaam).
Alle in de logbestanden geregistreerde gegevens worden alleen verzameld vanaf het begin van de logging.

Persoonsgegevens die mogelijk worden verwerkt tijdens service en onderhoud ter plaatse:
[Het type persoonsgegevens dat mogelijk toegankelijk is voor Konica Minolta technici is afhankelijk van de gegevens die op de Konica Minolta systemen worden verwerkt. Deze inhoud kan alleen door de Controller worden beoordeeld].

☒ Persoonlijke gegevens van de klant (bijv. voor- en achternaam)
☒ Communicatiegegevens van de klant (bijv. telefoon, e-mail)
☐ Basisgegevens van het contract (bijv. contractuele relatie, product/contractueel belang)
☐ Klantgeschiedenis (bijv. CRM-gegevens)
☐ facturatie- en betalingsgegevens
☐ Creditcardgegevens en bankgegevens (bankrekeningnummers)
☐ Planning- en controlegegevens
☐ Van derden verkregen informatie (bijv. kredietagentschappen, openbare registers)
☐ IP-adressen, MAC-adressen

Andere:

2.1.B) Aard van de persoonsgegevens bij Safe Q Cloud oplossingen:

Tijdens de levering en het gebruik van de Safe Q Cloud dienst heeft Konica Minolta toegang tot Persoonsgegevens van de Controller, zoals documentinhoud en metadata die een eindgebruiker verwerkt via de SafeQ Cloud Print-oplossing.
De gegevens bestaan uit drie hoofdcategorieën:

1. Documentinhoud

Document inhoud is de feitelijke documentinhoud die een eindgebruiker verwerkt via de SafeQ Cloud Print-oplossing. Dit type gegevens kan persoonlijke gegevens bevatten.

2. Metagegevens van documenten

Document Metagegevens bevatten informatie over afdruktaken (zie hieronder)

3. Toepassingsgegevens

Toepassing gegevens bevatten gebruikersnamen en bevatten de klantspecifieke configuratie van de geïnstalleerde oplossing.

De drie belangrijkste categorieën omvatten de volgende specifieke categorieën Persoonsgegevens van de Controller:

☒ Metagegevens van documenten (tijdstempel opdracht, eigenaar opdracht, bestandsnamen)
☒ IP-adressen, MAC-adressen
☒ IT-gebruikersnamen en andere unieke identificatiegegevens
☐ Persoonlijke stamgegevens (bijv. naam, adres)
☐ Communicatiegegevens (bijv. telefoon, e-mail)
☐ Stamgegevens contract (bijv. contractuele relatie, product/contractueel belang)
☐ Klantgeschiedenis (bijv. CRM-gegevens)
☐ Facturerings- en betalingsgegevens van contracten
☐ Creditcardgegevens en bankgegevens (bankrekeningnummers)
☐ Informatie verkregen van derden (bijv. kredietbureaus, openbare gegevensbestanden)
☐ Verder:

2.2. Categorieën van betrokkenen op wie de verwerking betrekking heeft:

[De volgende categorieën eigenaren van de onder 2 genoemde persoonsgegevens kunnen alleen door de verantwoordelijke voor de verwerking worden beoordeeld].

☒ Persoonsgegevens van werknemers van de controller (art. 88 GDPR)
☐ Persoonsgegevens van de business partner van de controller
☐ Persoonsgegevens van klanten van de controller

☐ Andere:

3. Subverwerkers

Konica Minolta Business Solutions Europe GmbH
Europaallee 17
30855 Langenhagen
Duitsland
Beschrijving van de opdracht:
- IT Service Provider voor Konica Minolta Business Solutions Belgium NV (inclusief exploitatie van Konica Minolta remote service en backup servers).
- 2nd Level Support op de printsystemen en Safe Q Cloud oplossing voor Konica Minolta Business Solutions Belgium
- De Safe Q Cloud oplossing wordt beheerd en gehost door Konica Minolta Europe in datacentra in Duitsland en Zweden die eigendom zijn van Konica Minolta Europe

YUSEN LOGISTICS (Benelux) BV
Middenweg 10
4782 PM Moerdijk
Nederland
Omschrijving van de opdracht:
- Logistieke dienstverlener (levering en installatie van de MFP's, harde schijf overschrijven en/of wissen na afloop van de Hoofdovereenkomst).

FOUNDEVER Operating Corporation Limited
Butts Road 53-55
Coventry - Warwickshire CV1 3 BH
England
Omschrijving van de opdracht:
-Callcenter voor elke aanvraag voor onderhoudsinterventies of leveringen van verbruiksartikelen aan klanten
- Konica Minolta informeert de Controller over het feit dat Engeland als onderdeel van het Verenigd Koninkrijk wordt beschouwd als een land met een adequaat niveau van gegevensbescherming in overeenstemming met het adequaatheidsbesluit van de Europese Commissie

I.S.A.B. NV
Huttegem 10,
8570 Anzegem
België
Beschrijving van de opdracht

- dienstverlener voor onderhoudsinterventies op de Konica Minolta systemen van sommige klanten

4. Technische en organisatorische beveiligingsmaatregelen

1. Geheimhouding

a) Fysieke toegangscontrole:

- Alleen personen die in het kader van hun takenpakket de persoonsgegevens moeten zien, worden geautoriseerd om persoonsgegevens te verwerken
- Er wordt vastgelegd welke functies dit zijn en hier wordt op gecontroleerd
- periodieke audits van toegangscontrole).
- Toegangscontrole in gebouwen van verwerker met badge inclusief serverruimte
- Documentatie van aanwezigheid in de serverruimten
- Toegangsregeling voor externe personen

b) Toegangscontrole Systemen en data:

De volgende maatregelen worden genomen om te voorkomen dat onbevoegden in de gegevensverwerkingssystemen binnendringen:

- Toegang tot de systemen is mogelijk na authenticatie met een individuele gebruikersnaam en wachtwoord
- Gebruik van complexe wachtwoorden met ten minste acht tekens die voldoen aan ten minste drie van de vier criteria (hoofdletter, kleine letter, cijfer, speciaal teken) en een verplichte wijziging van het wachtwoord om de 90 dagen.
- Verbod op bekendmaking van wachtwoorden
- Registratie van de toewijzing van toegangsrechten
- Beperking van de administratieve toegang tot het minimum
- Bescherming van gegevensverwerkende systemen tegen ongeoorloofde toegang door middel van passende firewallsystemen
- Automatische vergrendeling van systemen na een bepaalde periode van buitengebruikstelling
- Toewijzing van toegangsrechten op basis van een op behoeften gebaseerd autorisatieconcept
- Regelmatige controle van toegangsrechten
- Scheiding van autorisatierechten (organisatorisch) en toewijzing van rechten (technisch)

c) Controle op scheiding persoonsgegevens:

- Controles op pogingen tot ongeoorloofde toegang (IDS/IPS) (verplaatst van c)

- Specificatie van verschillende gebruikersprofielen (beheerders-/gebruikersniveaus)
- Specifieke toegangsrechten die overeenkomen met de vereisten voor gegevenstoegang
- Scheiding van productie- en testomgevingen door technische maatregelen (virtuele servers, gescheiden systemen, IP-adressegmentatie)

2. Integriteit

a) Controle van de overdracht:

- Encryptie van gegevensoverdracht, met name bij overdracht via openbare netwerken (bijv. SSL, TLS).
- Gegevensbeveiliging: wissen en/of vernietigen van gegevens, gegevensopslagapparatuur en afgedrukte kopieën volgens een concept van beschermingsklasse
- Encryptie van gegevensopslagmedia van werknemers (gsm, laptops, etc)
- Remote-wipe-optie voor mobiele apparaten (gsm)

b) Input controle:

- Toegangsrechten worden regelmatig gecontroleerd en bijgewerkt
- Logging van de gegevensverwerking maakt het mogelijk om later vast te stellen door wie persoonsgegevens zijn ingevoerd, gewijzigd of verwijderd (bv. logboeken voor gegevenswijzigingen in centrale ERP-systemen)
- Registratie van de acties die op systemen zijn uitgevoerd (bv. logbestanden)
- Excl. voor Printsystemen: Unieke identificatie en markering van gegevensopslag van MFP/PP-apparaten voor terugzending.

3. Beschikbaarheid en belastbaarheid: Controle van de beschikbaarheid en het vermogen tot herstel:

- Gebruik van twee gecertificeerde IT-centra die ver van elkaar verwijderd zijn, waardoor onderbreking van de dienstverlening door spiegeling wordt voorkomen (d.w.z. door het bewaren van redundante gegevens)
- Excl. voor Printsystemen:Technische voorzorgsmaatregelen in de vorm van systemen voor vroegtijdige waarschuwing ter bescherming tegen onderbrekingen door brand/hitte, water of oververhitting
- Excl. voor Printsystemen:Maatregelen ter bescherming tegen stroomuitval en stroomoverbelasting, bijvoorbeeld niet onderbreekbare stroomvoorzieningssystemen (UPS)
- Excl. voor Printsystemen:Geplande uitvoering van gegevensback-ups
- Gelaagde antivirus/firewall-architectuur
- Vastgesteld proces voor centrale aanschaf van hardware en software
- Mogelijkheid tot tijdig herstel (artikel 32, lid 1, onder c), van de GDPR) via een wereldwijd systeemgebonden back-upconcept.
- Regelmatige updates van alle gebruikte systemen, indien van toepassing
- Protocollen voor noodmaatregelen en gegevensherstel aanwezig

4. Opdrachtcontrole :

- Aanstelling van een functionaris voor gegevensbescherming
- GDPR-conforme inschakeling van externe dienstverleners
- Opleiding van werknemers bij de verwerking van persoonsgegevens
- Verplichte data beveiliging door werknemers
- Technische beveiliging door maatregelen voor toegangs-, scheidings- en invoercontroles

5. Controle van organisatie (verificatie, waardering en evaluatie):

- Processen voor continue controle en zo nodig aanpassing van de gegevensbeschermingsmaatregelen aanwezig
- Processen voor de behandeling van een inbreuk op gegevensbescherming zijn aanwezig
- Bedrijfsrichtlijnen voor de behandeling van persoonsgegevens en het gebruik van IT-systemen aanwezig
- Opleidingen voor werknemers omtrent IT security en AVG
- Beheer van incidenten (incident response management)