Verwerkersovereenkomst

Versie 2018.01

Deze Verwerkersovereenkomst is een bijlage bij de Hoofdovereenkomst (zoals gedefinieerd in artikel 1 van deze overeenkomt) tussen Klant en Minox B.V.

Partijen:

Klant:

_____, kantoorhoudende te _____,

statutair gevestigd te _____, ingeschreven in het handelsregister

onder KvK nr. _____, hierna “Klant” of “Verwerkingsverantwoordelijke”

En:

Minox B.V., kantoorhoudende te Lunet 3A, 3905 NW Veenendaal, statutair gevestigd te Veenendaal, ingeschreven in het handelsregister onder KvK nr. 30070920, hierna “Minox” of “Verwerker”

Overwegende dat:

- Partijen een overeenkomst hebben gesloten waarbij Verwerkingsverantwoordelijke gebruik maakt van het het cloud boekhoudpakket Minox Online dat Minox B.V. aan haar ter beschikking stelt;
- De Klant, Verwerkingsverantwoordelijke, beschikt over persoonsgegevens van diverse betrokkenen, waaronder, maar niet beperkt tot, financiële gegevens van eenmanszaken, vof’s, maatschappen en andere personenvennootschappen, persoonsgegevens van juridische vertegenwoordigers van andere juridische entiteiten, en gegevens van verkopen en betalingen aan personen die deze administreert in systemen die Minox ter beschikking stelt en die Klant heeft afgenomen, waaronder het boekhoudpakket Minox Online;
- Waar in deze overeenkomst verwezen wordt naar de Wet bescherming persoonsgegevens (Wbp), wordt vanaf 25 mei 2018 gedoeld op de corresponderende bepalingen uit de Algemene Verordening Gegevensbescherming (AVG). Indien er geen corresponderende bepaling bestaat, wordt de overeenkomst vanaf 25 mei 2018 op dit punt aangevuld.
- In deze overeenkomst leggen Partijen hun wederzijdse rechten en verplichtingen vast ten aanzien van het Verwerken van Persoonsgegevens met in achtneming van de geldende privacy regelgeving.

Partijen wensen ten behoeve van privacy protectie hun onderlinge rechten en plichten vast te leggen als volgt:

Artikel 1. Definities

In deze Overeenkomst wordt een aantal begrippen gebruikt, welke betekenis hieronder wordt verduidelijkt en welke definitie in lijn is met de definities die in de AVG voorkomen, omdat de AVG per 25 mei 2018 leidend is. De genoemde begrippen worden in deze Overeenkomst met een hoofdletter geschreven.

AVG	Algemene Verordening Gegevensbescherming, inclusief de uitvoeringswet van deze verordening. De AVG vervangt de Nederlands wet bescherming persoonsgegevens per 25 mei 2018. Daarnaast kunnen er guidelines van de artikel 29 Werkgroep van kracht worden die eveneens op deze Overeenkomst van toepassing zijn.
Beroeps- en gedragsregels:	De voor accountants geldende Beroeps- en gedragsregels (als vermeld op de website van de Nederlandse Beroepsorganisatie van Accountants, www.nba.nl)
Betrokkene:	Degene op wie een Persoonsgegeven betrekking heeft.
Verwerker:	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de Verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. In deze Overeenkomst is Minox aangemerkt als Verwerker.
Sub-verwerker:	Een andere verwerker die door de Verwerker wordt ingezet om ten behoeve van de Verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten.
Verwerkingsverantwoordelijke / Verantwoordelijke:	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In deze Overeenkomst is Klant aangemerkt als Verwerkingsverantwoordelijke ter zake van diens gegevens die hij/zij invoert in de software van Minox voor zover het persoonsgegevens betreft.
Bijzondere Persoonsgegevens:	Dit zijn gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele

	gerichtheid. Alsmede persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.
Datalek / Inbreuk in verband met persoonsgegevens:	Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot - of waarbij redelijkerwijs niet uit te sluiten valt dat die kan leiden tot - de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte Persoonsgegevens.
Derden:	Anderen dan Partijen en hun Medewerkers.
Hoofdovereenkomst:	De overeenkomst die tot stand is gekomen tussen Klant en Minox, bestaande uit een order van de Klant die tot stand komt hetzij via de website hetzij via telefonisch contact tezamen met de Algemene Voorwaarden onder welke Minox haar producten levert.
Meldplicht Datalekken:	De verplichting tot het melden van Datalekken aan de Autoriteit Persoonsgegevens en (in sommige gevallen) aan Betrokkene(n).
Medewerkers	Personen die werkzaam zijn bij Minox of bij Klant, ofwel in dienstbetrekking dan wel tijdelijk ingehuurd.
Onderliggende opdracht:	De opdracht zoals hierboven bedoeld in de overwegingen, oftewel de dienstverlening van Minox aan de Klant waarbij Minox haar boekhoudsoftware aan Klant ter beschikking stelt voor het doen van administraties zoals vastgelegd in de Hoofdovereenkomst
Overeenkomst:	Deze verwerkersovereenkomst, ookwel Verwerkersovereenkomst
Persoonsgegevens:	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de Betrokkene") die in het kader van de "Onderliggende opdracht" worden verwerkt; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Persoonsgegevens van gevoelige aard	Persoonsgegevens waarbij verlies of onrechtmatige Verwerking kunnen leiden tot (onder meer) stigmatisering of uitsluiting van Betrokkene, schade aan de gezondheid, financiële schade of tot (identiteits)fraude.

Tot deze categorieën van persoonsgegevens moeten in ieder geval worden gerekend:

- Bijzondere persoonsgegevens;
- Gegevens over de financiële of economische situatie van de Betrokkene;
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de Betrokkene;
- Gebruikersnamen, wachtwoorden en andere inloggegevens;
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude.

Verwerken / Verwerking: Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Artikel 2. Doeleinden van verwerking

2.1 Verwerker verbindt zich onder de voorwaarden van deze Overeenkomst in opdracht van Verwerkingsverantwoordelijke persoonsgegevens te verwerken. Verwerking zal uitsluitend plaatsvinden in het kader van de Hoofdovereenkomst die partijen zijn aangegaan plus de doeleinden die daarmee redelijkerwijs samenhangen of die met nadere instemming worden bepaald, te weten voor het in de 'cloud' verwerken van gegevens van Verwerkingsverantwoordelijke, en bijbehorende online diensten, in het bijzonder boekhouden in de ruimste zin van het woord in Minox Online. De Verwerking vind derhalve uitsluitend plaats onder verantwoordelijkheid van de Klant. Verwerker heeft geen zeggenschap over het doel en de middelen van de Verwerking en neemt geen beslissingen over de verwerkte gegevens in Minox Online.

Het gaat om de volgende soorten (persoons)gegevens:

- NAW gegevens;
- Persoonsgegevens die zijn opgenomen in documenten en welke in Minox Online worden verwerkt, bijvoorbeeld emailadressen of telefoonnummers;
- Betalingsgegevens en bankmutaties, waaronder IBAN en tenaamstellingsgegevens;
- Verkoopgegevens, waaronder afnemer en afgenomen producten en/of diensten;
- Inkoopgegevens, waaronder leverancier en geleverde producten en/of diensten;
- Financiële gegevens zoals omzet, kosten, bezittingen en schulden van eenmanszaken;
- BTW nummers;
- De dienstverlening die Verwerkingsverantwoordelijke is aangegaan met de betrokkene.

Het gaat om de volgende categoriën van betrokkenen:

- Medewerkers van de Verwerkingsverantwoordelijke;
- Klanten van de Verwerkingsverantwoordelijke;
- Leveranciers van de Verwerkingsverantwoordelijke;
- Overige relaties van de Verwerkingsverantwoordelijke (bijvoorbeeld donateurs of prospects).

2.2 De verwerking van persoonsgegevens vindt plaats onder verantwoordelijkheid van Klant. Minox heeft geen zeggenschap over het doel en de middelen van de Verwerking en neemt geen beslissing over zaken als het gebruik van Persoonsgegevens anders dan dat Minox het systeem ter beschikking stelt ten behoeve van het doen van administratie. Het doel van verwerking door Verwerker is uitvoering van de Hoofdovereenkomst met de Klant, namelijk de overeenkomst waarbij Verwerker een cloud boekhoudpakket ter beschikking heeft gesteld en zorgdraagt voor de werking en het onderhoud van het systeem en daaraan gerelateerde functies waaronder maar niet beperkt tot het verwerken van facturen en andere voor de boekhouding relevante documenten, het faciliteren van handmatige en geautomatiseerde boekingen, het verwerken van banktransacties en faciliteren van betalings- en incasso-opdrachten middels het boekhoudpakket. Wijzigingen in verwerkte persoonsgegevens worden uitsluitend gedaan door de Verwerkingsverantwoordelijke of op diens instructie.

2.3 De in opdracht van Verwerkingsverantwoordelijke te Verwerken persoonsgegevens blijven eigendom van Verwerkingsverantwoordelijke en/of de betreffende betrokkenen.

2.4 Verwerkingsverantwoordelijke heeft op grond van de voor haar als accountant geldende Beroeps- en gedragsregels (indien van toepassing) mogelijke verplichtingen en kan mogelijk daarbij Verwerker vragen om gegevens te verstrekken.

Artikel 3. Verplichtingen Verwerker

3.1 Ten aanzien van de in artikel 1 genoemde verwerkingen zal Verwerker zorg dragen voor de naleving van de toepasselijke wet- en regelgeving, waaronder in ieder geval begrepen de wet- en regelgeving op het gebied van de bescherming van persoonsgegevens, zoals de Wet bescherming persoonsgegevens, welke vanaf 25 mei 2018 wordt vervangen door de Algemene Verordening Gegevensbescherming (AVG).

3.2 Verwerker zal Verwerkingsverantwoordelijke, op diens eerste verzoek daartoe, informeren over de door haar genomen maatregelen aangaande haar verplichtingen onder deze Verwerkersovereenkomst.

3.3 De verplichtingen van de Verwerker die uit deze Verwerkersovereenkomst voortvloeien, gelden ook voor degenen die persoonsgegevens verwerken onder het gezag van Verwerker, waaronder begrepen maar niet beperkt tot werknemers, in de ruimste zin van het woord.

3.4 Verwerker verwerkt alle gegevens op instructie van Verwerkingsverantwoordelijke die immers in het systeem van Verwerker zelf alle gegevens invoert en/of die toestemming verleent voor systeemkoppelingen die gegevens uitwisselen met Minox Online. Indien er sprake is van een verwerking in strijd met de in lid 1 bedoelde wetgeving, informeert Verwerker terstond de Verwerkingsverantwoordelijke.

3.5. Voor zover mogelijk verleent Verwerker bijstand bij het vervullen van verplichtingen van de Verwerkingsverantwoordelijke om verzoeken om uitoefening van rechten van Betrokkenen af te handelen, zoals bij voorbeeld het recht op inzage.

Artikel 4. Doorgifte van persoonsgegevens

4.1 Verwerker mag de persoonsgegevens verwerken in landen binnen de Europese Unie (EU). Doorgifte naar landen buiten de Europese Unie wordt niet gedaan. Indien Verwerker dit in de toekomst wil veranderen, zal Verwerker de Verwerkingsverantwoordelijke hierover minimaal 3 maanden van te voren informeren en volgens de artikelen van de Algemene Verordening Gegevensbescherming (AVG) hiervoor een passend contract en passende maatregelen treffen zoals toegestaan door de AVG. De Verwerkingsverantwoordelijke kan hiertegen bezwaar maken.

4.2 Verwerker zal Verwerkingsverantwoordelijke melden om welk land of landen het gaat als er doorgifte plaatsvindt van gegevens naar andere landen binnen of buiten de Europese Unie (EU). Verwerker zal in ieder geval zorgdragen dat er een passend beschermingsniveau is dan wel er een EU-Modelovereenkomst is gesloten.

Artikel 5. Verdeling van verantwoordelijkheid

5.1 Verwerker stelt ten behoeve van de verwerkingen ICT-middelen ter beschikbaar die door Verwerkingsverantwoordelijke te gebruiken zijn voor de hierboven in artikellid 2.2. genoemde doelen. Verwerker verricht zelf alleen op basis van aparte afspraken verwerkingen.

5.2 Verwerker is louter verantwoordelijk voor de verwerking van de persoonsgegevens onder deze Verwerkersovereenkomst, overeenkomstig de instructies van Verwerkingsverantwoordelijke en onder de uitdrukkelijke (eind)verantwoordelijkheid van Verwerkingsverantwoordelijke. Voor de overige verwerkingen van persoonsgegevens, waaronder in ieder geval begrepen maar niet beperkt tot de verzameling van de persoonsgegevens door de Verwerkingsverantwoordelijke, verwerkingen voor doeleinden die niet door Verwerkingsverantwoordelijke aan Verwerker zijn gemeld, verwerkingen door derden en/of voor andere doeleinden, is Verwerker uitdrukkelijk niet verantwoordelijk.

5.3 Verwerker kan andere verwerkers (Sub-verwerkers) inschakelen voor het uitvoeren van bepaalde werkzaamheden die voortvloeien uit de Hoofdovereenkomst, bijvoorbeeld als deze Sub-verwerkers over specialistische kennis of middelen beschikken waarover verwerker niet beschikt. Als het inschakelen van Sub-verwerkers tot gevolg heeft dat deze persoonsgegevens gaan Verwerken dan zal Minox die Sub-verwerkers (schriftelijk) de verplichtingen uit deze Verwerkersovereenkomst opleggen. Met ondertekening van deze Verwerkersovereenkomst geeft Verwerkingsverantwoordelijke toestemming voor het inschakelen van de Sub-verwerkers die genoemd zijn in Bijlage I die bij deze Verwerkersovereenkomst hoort. Voor het inschakelen van overige Sub-verwerkers vraagt Verwerker eerst om toestemming van de Verwerkingsverantwoordelijke. Verwerkingsverantwoordelijke kan toestemming weigeren maar dit kan in sommige gevallen betekenen dat Verwerker de Hoofdovereenkomst niet naar behoren kan uitvoeren en moet beëindigen. Of een opdracht om deze reden moet worden beëindigd, is ter uitsluitende beoordeling aan Verwerker.

5.4 Verwerkingsverantwoordelijke garandeert dat de inhoud, het gebruik en de opdracht tot de verwerkingen van de persoonsgegevens zoals bedoeld in deze Verwerkersovereenkomst, niet onrechtmatig zijn en geen inbreuk maken op enig recht van derden.

Artikel 6. Beveiliging

6.1 Verwerker neemt technische en organisatorische maatregelen met betrekking tot de te verrichten verwerkingen van persoonsgegevens, tegen verlies of tegen enige vorm van onrechtmatige verwerking (zoals onbevoegde kennisname, aantasting, wijziging of verstrekking van de persoonsgegevens).

6.2 Indien een uitdrukkelijk omschreven beveiliging in de Verwerkersovereenkomst ontbreekt, zal Verwerker zich inspannen dat de beveiliging zal voldoen aan een niveau dat, gelet op de stand van de techniek, de gevoeligheid van de persoonsgegevens en de aan het treffen van de beveiliging verbonden kosten, niet onredelijk is en voldoet aan de geldende regelgeving.

6.3 Verwerker heeft onverminderd de verplichtingen uit de vorige leden, in ieder geval de volgende maatregelen genomen:

a. logische toegangscontrole, gebruik makend van gebruikersnaam en wachtwoord welke encrypted wordt opgeslagen;

b. organisatorische maatregelen voor toegangsbeveiliging, waarbij op grond van autorisaties toegang wordt verleend en Verwerker daarnaast haar medewerkers bij aanname verzoekt een Verklaring omtrent gedrag (VOG) in te leveren om integriteit te waarborgen;

c. beveiliging van netwerkverbindingen via Secure Socket Layer (SSL) of Transport Layer Security (TLS) technologie;

d. encrypted opslag van persoonsgegevens in databases (AWS RDS);

e. ISO certificering cloud hosting partner Amazon (AWS): ISO 27001, ISO 27017, ISO 27018, ISO 9001 en inloggen in AWS console met 2-factor authenticatie;

f. regelmatige automatische backups, minimaal elke nacht.

In Bijlage II staat een lijst van verdere beveiligingsmaatregelen.

6.4 Verwerkingsverantwoordelijke voert zelf persoonsgegevens in in het systeem van Verwerker en/of verleent zelf toestemming voor systeemkoppelingen die gegevens uitwisselen met Minox Online, en is daarom zelf verantwoordelijk voor de correctheid van de ingevoerde of aangeleverde gegevens, het eventueel informeren van betrokkenen en het zorgdragen dat de logische toegangscontrole uitsluitend toegankelijk is voor diens werknemers en dat alleen diegenen hiertoe toegang krijgen die Verwerkingsverantwoordelijke geautoriseerd heeft. Daarnaast heeft Verwerkingsverantwoordelijke een eigen verplichting om de logische toegangscontrole ontoegankelijk te houden voor derden, zoals wachtwoorden te beschermen en zorg te dragen voor processen in zijn eigen bedrijf die beveiliging van het systeem bevorderen.

Artikel 7. Meldplicht

7.1 In het geval van de ontdekking van een Beveiligingslek (een tekortkoming in of de inbreuk op de beveiliging van persoonsgegevens) en/of een Datalek (een inbreuk op de beveiliging van persoonsgegevens die leidt tot een aanzienlijke kans op nadelige gevolgen, dan wel nadelige gevolgen heeft), voor de bescherming van persoonsgegevens als bedoeld in artikel 34a lid 1 Wbp c.q. artikelen 33 en 34 AVG, zal Verwerker de Verwerkingsverantwoordelijke hierover zo snel mogelijk, in ieder geval binnen 24 uur na ontdekking, informeren. Naar aanleiding hiervan, zal de Verwerkingsverantwoordelijke beoordelen of deze de betrokkenen en/of Autoriteit Persoonsgegevens (AP) zal informeren of niet.

7.2 De meldplicht behelst in ieder geval het melden van het feit dat er een lek is geweest. Daarnaast behelst de meldplicht, voor zover deze informatie bij Verwerker beschikbaar is:

- Wat de (vermeende) oorzaak van het lek is;
- Wat het (vooralsnog) bekende en/of te verwachten gevolg is;
- Wat de (voorgestelde) oplossing is;
- Contactgegevens voor de opvolging van de melding;
- Het aantal personen van wie gegevens zijn gelekt (indien geen exact aantal bekend is, minimale en maximale aantallen van personen van wie gegevens zijn gelekt);
- Soort of soorten persoonsgegevens die gelekt zijn;
- Omschrijving van de groep personen van wie gegevens zijn gelekt, voor zover dit mogelijk is;
- Datum of periode waarbinnen het lek heeft plaatsgevonden;

- Datum waarop het lek bekend is geworden bij de Verwerker;
- Of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden;
- Wat de voorgenomen en/of reeds genomen maatregelen zijn om het lek te dichten en om de gevolgen van het lek te beperken.

Indien Verwerker op het moment van de melding nog niet over de bovenstaande informatie beschikt, zal Verwerker dit zo gauw mogelijk nasturen.

Artikel 8. Afhandeling verzoeken van betrokkenen

8.1 In het geval dat een betrokkene een verzoek met betrekking tot zijn persoonsgegevens richt aan Verwerker, zal Verwerker het verzoek doorsturen aan Verwerkingsverantwoordelijke, en zal Verwerkingsverantwoordelijke het verzoek verder afhandelen. Verwerker mag de betrokkene daarvan op de hoogte stellen. Voor zover mogelijk zal Verwerker de Verwerkingsverantwoordelijke assisteren bij het vervullen van de verplichtingen van Verwerkingsverantwoordelijke om verzoeken om uitoefening van de rechten van Betrokkenen af te handelen, voor zover het systeem dat Verwerker ter beschikking stelt hierbij een rol speelt.

Artikel 9. Geheimhouding en vertrouwelijkheid

9.1 Op alle persoonsgegevens die Verwerker van Verwerkingsverantwoordelijke ontvangt en/of zelf verzamelt in het kader van deze Verwerkersovereenkomst, rust een geheimhoudingsplicht jegens derden. Verwerker zal deze informatie niet voor een ander doel gebruiken dan waarvoor zij deze heeft verkregen, zelfs niet wanneer deze in een zodanige vorm is gebracht zodat deze niet tot betrokkenen herleidbaar is.

9.2 Deze geheimhoudingsplicht is niet van toepassing voor zover Verwerkingsverantwoordelijke uitdrukkelijke toestemming heeft gegeven om de informatie aan derden te verschaffen, indien het verstrekken van de informatie aan derden logischerwijs noodzakelijk is gezien de aard van de verstrekte opdracht en de uitvoering van deze Verwerkersovereenkomst, of indien er een wettelijke verplichting bestaat om de informatie aan een derde te verstrekken.

Artikel 10. Audit

10.1 Indien er een verplichting bestaat om op het systeem dat Verwerker ter beschikking stelt een audit uit te voeren, zal Verwerker zorgdragen dat dit mogelijk wordt gemaakt.

Artikel 11. Aansprakelijkheid

11.1 Op grond van artikel 82 AVG is Verwerker alleen aansprakelijk voor schade van de Betrokkene indien Verwerker aantoonbaar verantwoordelijk is voor het schadeveroorzakende feit en voor zover deze gehandeld heeft buiten de instructies van de Klant c.q. Hoofdovereenkomst die Verwerker gesloten heeft met de Verwerkingsverantwoordelijke. Verwerker is aansprakelijk voor schade van de Verwerkingsverantwoordelijke als gevolg van een toerekenbare tekortkoming in de nakoming van de Verwerkersovereenkomst, dan wel uit onrechtmatige daad of anderszins, tot een maximum van 1 jaar omzet die de Verwerker van de Klant heeft ontvangen ten tijde van de schade dan wel tot het bedrag dat de verzekeraar uitkeert. Schadevergoeding per gebeurtenis (een reeks opeenvolgende gebeurtenissen geldt als één gebeurtenis) is beperkt tot de vergoeding van directe schade.

11.2.1 Onder directe schade wordt uitsluitend verstaan alle schade bestaande uit:

a. schade direct toegebracht aan stoffelijke zaken (“zaakschade”);

b. redelijke en aantoonbare kosten om de Verwerker er toe te manen de Verwerkersovereenkomst (weer) deugdelijk na te komen;

c. redelijke kosten ter vaststelling van de oorzaak en de omvang van de schade voor zover betrekking hebbende op de directe schade zoals hier bedoeld is; en

d. redelijke en aantoonbare kosten die Verwerkingsverantwoordelijke heeft gemaakt ter voorkoming of beperking van de directe schade zoals in dit artikel bedoeld.

11.3 De aansprakelijkheid van Verwerker voor indirecte schade is uitgesloten. Onder indirecte schade wordt verstaan alle schade die geen directe schade is en daarmee in ieder geval, maar niet beperkt tot, gevolgschade, gederfde winst, gemiste besparingen, verminderde goodwill, schade door bedrijfsstagnatie, schade door het niet bepalen van marketingdoeleinden, schade verband houdende met het gebruik van door Verwerkingsverantwoordelijke voorgeschreven gegevens of databestanden, of verlies, verminking of vernietiging van gegevens of databestanden.

11.4 De in dit artikel bedoelde uitsluitingen en beperkingen komen te vervallen indien en voor zover de schade het gevolg is van opzet of bewuste roekeloosheid van Verwerker of haar bedrijfsleiding.

11.5 Tenzij nakoming door Verwerker blijvend onmogelijk is, ontstaat de aansprakelijkheid van Verwerker wegens toerekenbare tekortkoming in de nakoming van de Overeenkomst slechts indien Verwerkingsverantwoordelijke de Verwerker onverwijld schriftelijk in gebreke stelt, waarbij een redelijke termijn voor de zuivering van de tekortkoming wordt gesteld, en Verwerker ook na die termijn toerekenbaar blijft tekortschieten in de nakoming van haar verplichtingen. De ingebrekestelling dient een zo volledig en gedetailleerd mogelijke omschrijving van de tekortkoming te bevatten, opdat Verwerker in de gelegenheid wordt gesteld adequaat te reageren.

11.6 Iedere vordering tot schadevergoeding door Verwerkingsverantwoordelijke tegen Verwerker die niet gespecificeerd en expliciet is gemeld, vervalt door het enkele verloop van twaalf (12) maanden na het ontstaan van de vordering.

Artikel 12. Duur en beëindiging

12.1 Deze Verwerkersovereenkomst komt tot stand door ondertekening van Partijen en wel op de datum van de laatste ondertekening en is van toepassing op iedere Verwerking die door Minox als Verwerker wordt gedaan op basis van de Onderliggende Opdracht.

12.2 Deze Verwerkersovereenkomst is aangegaan voor onbepaalde tijd. Hierbij dient een opzegtermijn van drie maanden in acht te worden genomen. Beëindiging van de Hoofdovereenkomst doet echter deze Verwerkersovereenkomst op hetzelfde moment eindigen.

12.3 Zodra de Verwerkersovereenkomst, om welke reden en op welke wijze dan ook, is beëindigd, zal Verwerker indien verzocht door de Verwerkingsverantwoordelijke alle persoonsgegevens die bij haar aanwezig zijn in originele of kopievorm retourneren aan Verwerkingsverantwoordelijke, en daarna deze en eventuele kopieën daarvan verwijderen en/of vernietigen.

12.4 Deze Verwerkersovereenkomst mag worden gewijzigd op dezelfde wijze als de Hoofdovereenkomst.

12.5 Na het eindigen van deze Verwerkersovereenkomst blijven artikelen 11 en 9 van kracht.

Artikel 13. Slotbepalingen en toepasselijk recht

13.1 De Verwerkersovereenkomst en de uitvoering daarvan worden beheerst door Nederlands recht.

13.2 Alle geschillen, die tussen Partijen ontstaan in verband met de Verwerkersovereenkomst, zullen worden voorgelegd aan de bevoegde rechter te Utrecht, tenzij de wet dwingend anders voorschrijft.

13.3 Als één of meerdere bepalingen in deze Overeenkomst niet geldig blijken te zijn, dan heeft dit geen gevolgen voor de geldigheid van de overige bepalingen in deze Overeenkomst. Deze ongeldige bepaling(en) zullen dan worden vervangen door een andere bepaling zoveel als mogelijk in de geest is van de ongeldige bepaling, maar dan uiteraard zo vormgegeven dat de bepaling wel geldig is.

13.4 Mededelingen in het kader van deze Overeenkomst (inclusief mededelingen in het kader van artikel 6 – Meldplicht) zullen door Verwerker en Verwerkingsverantwoordelijke worden gedaan aan onderstaande Medewerkers:

Hessel Kuik
Minox B.V.
hessel@minox.nl
06-46387825

Aldus overeengekomen en getekend op _____ te _____,

Klant:	_____	Minox B.V.
Naam:	_____	Hessel Kuik
Functie:	_____	CEO
Handtekening:		Handtekening:

Bijlage I. Overzicht van sub-verwerkers

ID	Marktpartij	Dienst
1.	Go2UBL	Herkenning en omzetting van documenten naar digitale bestanden, bijvoorbeeld gescande inkoop- en/of verkoopfacturen naar UBL (onderdeel van Minox 'Scan & Herken').
2.	TriFact 365	Herkenning en omzetting van documenten naar digitale bestanden, bijvoorbeeld gescande inkoop- en/of verkoopfacturen naar UBL (onderdeel van Minox 'Scan & Herken').
3.	Storecove	Koppeling met portals van leveranciers om inkoopfacturen automatisch op te halen (onderdeel van Minox 'Factuurconnectie'). Minox slaat zelf niet de ingevoerde gebruikersnaam en wachtwoord op, maar geeft de ingevoerde gegevens alleen door aan Storecove.
4.	Creaim	Minox koppelt met Creaim voor het doorsturen van BTW en ICP aangiftes en suppleties naar de Belastingdienst. Gebruikers dienen een eigen account te hebben bij Creaim om deze dienst te kunnen gebruiken.
5.	Mailgun	Minox maakt gebruik van de online diensten van Mailgun om e-mails vanuit Minox te versturen en te ontvangen.
6.	Bizcuit	Minox maakt gebruik van de Bizcuit app van gelieerde onderneming Bizcuit B.V. Gegevens die worden uitgewisseld hebben betrekking op gebruikers (en hun rechten), banktransacties (indien gekoppeld), betalings- en incasso-opdrachten (indien gekoppeld), documenten (indien gekoppeld). De uitwisseling van gegevens zal worden uitgebreid om meer diensten te kunnen leveren aan Minox en Bizcuit gebruikers. Er zal om expliciete toestemming gevraagd worden indien er functionaliteiten worden gebruikt waarbij uitwisseling van gegevens plaats zal vinden, waarbij de gebruiker zal worden geïnformeerd over welke gegevens uitgewisseld zullen worden en waarom.
7.	Diverse koppelpartners	Minox biedt een zogenaamde Open API, wat betekent dat marktpartijen hun applicaties en/of diensten kunnen aanbieden in combinatie met Minox (bijvoorbeeld een koppeling van een kassasysteem aan Minox). Tijdens het proces van koppelen zal expliciet om toestemming gevraagd worden om gegevens met Minox uit te wisselen, waarbij de gebruiker zal worden geïnformeerd over welke gegevens uitgewisseld zullen worden en waarom. De gebruiker dient de toestemming van kracht te maken door zijn/haar inloggegevens in te voeren. Dit zorgt er voor dat de toestemming en rechten van de gebruiker gebruikt worden voor het opzetten van de koppeling. Voorbeelden: Kassasystemen, webshops, rapportagepakketten, salarispakketten, uren- en projectensoftware.

8.	Amazon Web Services (AWS)	Minox maakt gebruik van AWS voor het hosten van haar cloud diensten. Alle gegevens worden opgeslagen in de cloud bij Amazon (gebruik makend van o.a. de AWS RDS en S3 diensten), waarbij de data altijd opgeslagen wordt op servers in Europa. Hoewel Amazon een Amerikaans bedrijf is, biedt ze de garantie dat de Minox data op Europees grondgebied staat en blijft staan. AWS is compliant met EU General Data Protection / GDPR wetgeving, zie voor meer informatie: https://aws.amazon.com/compliance/eu-data-protection https://aws.amazon.com/compliance/eu-us-privacy-shield-faq Daarmee heeft de Amerikaanse overheid geen toestemming om toegang te hebben tot de Minox data[1]. Ook is alle data tijdens transport en opslag volledig versleuteld. Minox hecht veel waarde aan de bescherming van de data van haar klanten en houdt de ontwikkelingen (o.a. ook in het kader van de AVG) goed in de gaten.
9.	Teamviewer	Minox Customer Support maakt gebruik van de applicatie Teamviewer om remote support te leveren aan Minox klanten. Teamviewer heeft geen toegang tot de data in Minox, maar de video stream waarin mogelijk Minox schermen met daarop zichtbaar persoonsgegevens loopt over de servers van Teamviewer. Om deze reden is Teamviewer voor de volledigheid in dit overzicht opgenomen.
10.	Lokaal geïnstalleerde applicaties en het Minox lokale netwerk	Minox Customer Support kan voor het leveren van support aan Minox klanten mogelijk gegevens exporteren naar bestanden buiten de Minox applicatie voor verdere analyse of om te delen met de klant. Voorbeelden zijn exports van facturen of rapporten, welke geopend worden in Microsoft Word, Microsoft Excel, Acrobat Reader of andere online of offline toepassingen van derden. Het exporteren en openen van bestanden die data van klanten bevatten zal alleen gebeuren op verzoek van de betreffende klant, en deze gegevens worden alleen bewaard binnen het beveiligde lokale netwerk van Minox (LAN), en alleen voor de duur van het klantverzoek. De gegevens worden dus weer verwijderd na het afronden van de support voor het betreffende klantverzoek.
11.	Email / Microsoft Exchange Online	In aansluiting op het punt hierboven is het mogelijk dat Minox Customer Support via email gegevens ontvangt van, of verstuurd naar, Minox klanten. Het is hierbij mogelijk dat de gegevens persoonsgegevens omvatten. Minox maakt hierbij gebruik van de Microsoft Exchange Online diensten. Deze mails worden verwijderd uit de Verzonden Items na verzending.
12.	MailChimp	Minox klanten hebben de mogelijkheid om één of meerdere nieuwsbrieven te ontvangen van Minox. Deze nieuwsbrieven worden verzonden op basis van emaillijsten welke worden bijgehouden in de cloud applicatie MailChimp. Ontvangers van een nieuwsbrief hebben te allen tijde de mogelijkheid om zich voor de betreffende nieuwsbrief af te melden met onmiddellijke ingang.

[1] Uitkomst van een eerdere zaak die Microsoft succesvol tegen de Amerikaanse overheid heeft aangespannen, is geweest dat de data die zich op Europees grondgebied bevond, niet hoefde te worden verschaft aan de Amerikaanse overheid. Zie bijvoorbeeld: Blog

Uiteraard is dit een specifieke uitspraak en kan er geen 100% uitsluitsel over alle mogelijke gevallen gegeven worden, maar vooralsnog is dit hoe de wetgeving hier uitspraken over gedaan heeft.

Het tweede aspect is of de Amerikaanse overheid, toegang kan krijgen tot de data. Dit is een technische restrictie gebaseerd op data encryptie. Ook hier geldt dat 100% uitsluitsel niet te geven is. Wel is het naar de mening van Minox onwaarschijnlijk dat Amazon zal meewerken aan het verstrekken van een encryptie key aan de Amerikaanse overheid. Ook is het naar de mening van Minox onwaarschijnlijk dat de Amerikaanse overheid de AWS encryptie zal hacken en in strijd zal handelen met eerdere gerechtelijke uitspraken. Mocht er een indicatie komen dat er veranderingen zijn op dit vlak (richting Minox of andere cloud service providers), dan zal Minox haar klanten hierover informeren.

13.	Jonar	Jonar is een in Canada gevestigde onderneming die het product Paragon ERP op de markt brengt. Minox maakt gebruik van dit product indien Minox ERP door een klant wordt afgenomen (Minox ERP is een bundel van Minox Xtra voor de financiële administratie en Paragon voor de ERP processen zoals bijvoorbeeld ordermanagement, voorraadbeheer, logistiek, planning en productie). Het product Paragon kan hierbij whitelabel worden gebruikt. Voor Minox ERP klanten (daarmee zijnde Paragon gebruikers) is Jonar sub-verwerker.
14.	Google Cloud	Minox ERP (uitvoeringen Handel, Handel Pro en Productie) maakt gebruik van Google Cloud voor het hosten van haar cloud diensten. Alle gegevens uit het ERP gedeelte van Minox ERP worden opgeslagen in de cloud bij Google, waarbij de data altijd opgeslagen wordt op servers in Europa. Hoewel Google een Amerikaans bedrijf is, biedt ze de garantie dat de Minox ERP data op Europees grondgebied staat en blijft staan. Google is compliant met EU General Data Protection / GDPR wetgeving, zie voor meer informatie: https://cloud.google.com/security/compliance/eu-data-protection https://privacy.google.com/businesses/compliance Zie ook Google en AVG: https://www.google.com/intl/nl/cloud/security/gdpr Daarmee heeft de Amerikaanse overheid geen toestemming om toegang te hebben tot de Minox ERP data[2]. Ook is alle data tijdens opslag volledig versleuteld. Minox hecht veel waarde aan de bescherming van de data van haar klanten en houdt de ontwikkelingen (o.a. ook in het kader van de AVG) goed in de gaten. Voor Minox ERP klanten is Google sub-verwerker.

[2] *Uitkomst van een eerdere zaak die Microsoft succesvol tegen de Amerikaanse overheid heeft aangespannen, is geweest dat de data die zich op Europees grondgebied bevond, niet hoefde te worden verschaft aan de Amerikaanse overheid. Zie bijvoorbeeld: Blog*

Uiteraard is dit een specifieke uitspraak en kan er geen 100% uitsluitsel over alle mogelijke gevallen gegeven worden, maar vooralsnog is dit hoe de wetgeving hier uitspraken over gedaan heeft.

Het is naar de mening van Minox onwaarschijnlijk dat de Amerikaanse overheid in strijd zal handelen met eerdere gerechtelijke uitspraken. Mocht er een indicatie komen dat er veranderingen zijn op dit vlak (richting Minox of andere cloud service providers), dan zal Minox haar klanten hierover informeren.

Bijlage II. Beveiligingsmaatregelen

Onderstaande tabel bevat een overzicht van de belangrijkste beveiligingsmaatregelen die uiterlijk vanaf 25 mei 2018 effectief zijn voor Minox Online en/of Minox ERP.

ID	Beveiligingsmaatregel	Minox Online	Minox ERP
1.	Encryptie data verkeer (SSL, TLS).	X	X
2.	Encryptie data opslag (Amazon RDS, Amazon S3).	X	
3.	Inloggen in applicatie met persoonsgebonden account gegevens (klantnummer, gebruikersnaam, wachtwoord). NB. Minox is niet verantwoordelijk voor situaties waarin klanten account gegevens delen met meerdere personen. Dit wordt beschouwd als onbedoeld gebruik.	X	X
4.	ISO certificering hosting partner Amazon (AWS): ISO 27001, ISO 27017, ISO 27018, ISO 9001.	X	
5.	ISO certificering hosting partner Google Cloud: ISO 27001, ISO 27017, ISO 27018.		X
6.	OTAP straat met restrictie toegang tot Ontwikkel, Test, Acceptatie en Productie omgeving(en). Alleen een beperkt aantal bevoegde Minox werknemers hebben toegang. Het aantal medewerkers met back-end toegang tot de Productie omgeving(en) zal te allen tijden beperkt worden tot het minimum dat nodig is om te voorzien in de behoeften voor onderhouds-, update- en issue resolutie processen.	X	X
7.	Er wordt gebruik gemaakt van een bastion server voor gecontroleerde toegang tot de Productie omgeving(en). Deze 'special purpose' server wordt gebruikt door systemadminstrators om (middels 2-factor autenticatie) toegang te krijgen tot de Productie omgeving(en), en wordt uitgeschakeld op momenten dat die toegang niet nodig is. Dit betekent dat de mogelijkheid om de Productie omgeving(en) te benaderen het grootste deel van de tijd niet beschikbaar is. Dit is in zichzelf een toegangsbeveiligingsmaatregel.	X	
8.	Een Verklaring omtrent gedrag (VOG) is vereist voor Minox medewerkers en directie, waaruit blijkt dat gedrag in het verleden geen bezwaar vormt voor het vervullen van de betreffende taak of functie. Daarnaast zijn er geheimhoudingsverklaringen van kracht voor alle medewerkers en inhuurkrachten. NB. De VOG beveiligingsmaatregel is niet van toepassing op (alle) sub-verwerkers, mede omdat het concept van de VOG in Canada niet van toepassing is, waardoor dit niet van toepassing is op Jonar (sub-verwerker in het kader van Minox ERP).	X	X

9.	Restrictie toegang tot Amazon (AWS) root accounts is beperkt tot de hoofdverantwoordelijke.	X	
10.	Inloggen in AWS console met 2-factor authentication (cedentials, authenticator app).	X	
11.	Bij wijzigingen in klantgegevens (stamdata of transacties) wordt altijd de account en het tijdstip van de laatste wijziging vastgelegd op het record.	X	X
12.	Alleen medewerkers met support of root cause analysis (RCA) rollen hebben een persoonsgebonden account met uitgebreide rechten op de Productie omgeving(en). Deze Minox medewerkers hebben de mogelijkheid persoonsgegevens in te zien, maar dit gebeurt uitsluitend op verzoek van de Verwerkingsverantwoordelijke (bijvoorbeeld in het kader van customer support) of indien er sprake is van een 'quality of service' melding. Dit laatste betreft systeemmeldingen als gevolg van datacontroles, welke periodiek (bijvoorbeeld de nachtelijke routine controles) en ad hoc (bijvoorbeeld na een data migratie of als onderdeel van debugging) worden uitgevoerd. Minox medewerkers die inloggen in Minox Online met een gebruikersaccount met uitgebreide rechten worden vanuit het systeem verplicht om per administratie per inlog de reden op te geven waarom er wordt ingelogd (standaard categorie plus toelichting). Bij beëindiging van het dienstverband wordt de betreffende persoonsgebonden account verwijderd of inactief gemaakt.	X	
13.	Test omgeving(en) bevatten geen Productie data.	X	X
14.	Acceptatie omgeving(en) bevatten geen Productie data. NB. Om acceptatietesten te kunnen doen met representatieve data is het wel mogelijk dat Productiedata in de Productie omgeving(en) wordt geanonimiseerd, waarna deze in zijn geheel of in delen naar Acceptatie omgeving(en) kunnen worden gekopieerd. Persoonsgegevens (en andere herleidbare gegevens) worden hierbij volledig onherkenbaar gemaakt.	X	X
15.	De applicatie is voorzien van rol-gebaseerde toegang tot functionaliteiten en data in de applicatie.	X	X
16.	Koppelingen (middels API's) van buitenaf zijn beveiligd middels OAuth. De klant of een door de klant geautoriseerde accountant geeft expliciete toestemming om de koppelpartner de mogelijkheid te geven om specifieke verwerkingen uit te voeren.	X	X
17.	Databases waarin persoonsgegevens vastliggen zijn gescheiden per klant. Daarnaast worden gescheiden systeem accounts gebruikt voor het uitvoeren van queries op de databases.	X	X
18.	Minox Online wordt regelmatig onderworpen aan penetratie (PEN) testen door een externe partij.	X	

19.	Er worden nooit gegevens uit een klantadministratie of over gebruikers of wachtwoorden gedeeld via telefoon of email, IM, intranet, extranet, netwerkschijf of andere applicaties van derden, met uitzondering van informatie die op verzoek van de betreffende klant wordt verzonden naar het bij ons bekende emailadres van de klant (emailadres gebruikt bij aanmelding).	X	`X
20.	Bij gebruik van data over administraties heen voor analytische toepassingen of bijvoorbeeld AI, worden (verwijzingen naar) persoonsgegevens weggelaten. Data voor dergelijke toepassingen wordt dus alleen anoniem (en over het algemeen geaggregeerd) gebruikt.	X	X
21.	Er is per medewerker of bevoegde externen individuele een alarm code voor toegang tot het Minox kantoorpand. Bij beëindiging van het dienst- of samenwerkingsverband wordt de betreffende code uit het alarmsysteem verwijderd. Toegang tot het kantoorpand is eveneens beveiligd middels sloten. Er is een sleutelregister dat actief wordt bijgehouden. Bij beëindiging van het dienst- of samenwerkingsverband worden sleutels direct ingeleverd.	X	X
22.	Toegang tot het interne CRM applicatie is beveiligd middels netwerk toegang (de gebruiker moet zich binnen het Minox LAN bevinden, dus op kantoor of via VPN verbinding). De applicatie is voorzien van rol-gebaseerde toegang tot functionaliteiten en data in de applicatie. Gebruikers met uitgebreide toegang hebben accounts die extra beveiligd zijn met wachtwoorden.	X	X