Ondergetekenden:

1. Afnemer van de Software, hierna te noemen "**Verwerkingsverantwoordelijke**"; en

2. Smart Production Solutions B.V., statutair gevestigd en kantoorhoudende te 's-Hertogenbosch aan Utopialaan 36 (5232 CE), hierbij rechtsgeldig vertegenwoordigd door de heer E. Klement, hierna te noemen: "**Verwerker**"; en

Overwegende dat:

a) Verwerker stelt software voor de maakindustrie beschikbaar aan Verwerkingsverantwoordelijke in de vorm van Sofware as Service (SaaS) op basis van de overeengekomen afspraken in de initiële overeenkomst.
b) Het verrichten van deze diensten brengt met zich dat persoonsgegevens worden verwerkt. Verwerkingsverantwoordelijke is de verwerkingsverantwoordelijke voor deze persoonsgegevens, hetgeen inhoudt dat zij doel en middelen vaststelt. Verwerker heeft te gelden als verwerker van deze persoonsgegevens, hetgeen inhoudt dat zij uitsluitend conform de opdracht en instructie van verwerkingsverantwoordelijke zal handelen.
c) Partijen wensen middels deze verwerkersovereenkomst de afspraken met betrekking tot de verwerking van persoonsgegevens in het kader van de hierboven bedoelde diensten vast te leggen.

Komen het volgende overeen:

1 DEFINITIES

1.1 In deze overeenkomst hebben de volgende (onderstreepte) begrippen de daaropvolgende betekenis:

a.) Aanvullende Nationale Wetgeving: elke wetgeving met betrekking tot de verwerking van persoonsgegevens in een lidstaat van de EU, naast de AVG.
b.) Diensten: de diensten die door Verwerker voor Verwerkingsverantwoordelijke worden verricht op basis van een Dienstverleningsovereenkomst.
c.) Dienstverleningsovereenkomst: overeenkomst tussen Verwerker en Verwerkingsverantwoordelijke die betrekking heeft op het verrichten van Diensten.
d.) Implementatiewetgeving: de toepasselijke nationale wetgeving die in het betreffende land van toepassing is op de verwerking van persoonsgegevens in het kader van de Diensten, waaronder de wetgeving die is geïmplementeerd om uitvoering te geven aan de Privacyrichtlijn.
e.) AVG: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
f.) Inbreuk: de Inbreuk In Verband Met Persoonsgegevens zoals gedefinieerd in de Privacy verordening.
g.) Sub-Verwerker: iedere derde partij die door Verwerker is betrokken bij de verwerking van persoonsgegevens in het kader van de Diensten.
h.) Toepasselijke Privacy Wetgeving: de Privacy verordening en de Aanvullende Nationale Wetgeving van de betreffende landen.

1.2 Elk begrip dat hier niet is gedefinieerd, maar dat wel is gedefinieerd in de Toepasselijke Privacy Wetgeving (zoals "*persoonsgegeven*", "*verwerken*", etc.), heeft in deze overeenkomst dezelfde betekenis als in de Toepasselijke Privacy Wetgeving.

1.3 Voor wat betreft de begrippen wordt in deze overeenkomst de terminologie van de Privacy verordening gebruikt (*bijv. "verwerker" i.p.v. "bewerker"*). Daarmee wordt niet bedoeld af te wijken van de betekenis van de Toepasselijke Privacy Wetgeving.

2 ALGEMEEN

2.1 Deze verwerkersovereenkomst is een bijlage bij- en maakt deel uit van de Dienstverleningsovereenkomst(en).

2.2 Deze verwerkersovereenkomst heeft betrekking op de verwerking van persoonsgegevens die uit de Diensten voortvloeit, ongeacht of de betreffende Dienstverleningsovereenkomst wel of niet expliciet refereert aan de verwerking van persoonsgegevens.

2.3 De aard en de doeleinden van de verwerking, evenals het soort persoonsgegevens en de categorieën van betrokkenen die door Verwerker namens Verwerkingsverantwoordelijke worden verwerkt, staan nader uitgewerkt in Bijlage 1, bij gebreke waarvan de verwerking is beperkt tot de werkzaamheden die strikt noodzakelijk zijn voor de uitvoering van de Dienstverleningsovereenkomst.

3 HOEDANIGHEDEN EN TAKEN VAN PARTIJEN

3.1 Verwerker zal alleen op basis van schriftelijke instructies van Verwerkingsverantwoordelijke de persoonsgegevens verwerken.

3.2 Verwerkingsverantwoordelijke wordt geacht de instructies aan Verwerker te hebben gegeven voor elke verwerking die strikt noodzakelijk is in het kader van het verlenen van de Diensten. Onder deze instructies zijn mede begrepen wijzigingen aan de Diensten, voor zover de Dienstverleningsovereenkomst zulke wijzigingen toestaat.

3.3 De Verwerkingsverantwoordelijke garandeert de rechtmatigheid van het gebruik, de verwerking, de archivering, het doel van het gebruik en de uitwisseling van de Persoonsgegevens en/of ieder ander gebruik, zoals die voortvloeien uit de tenuitvoerlegging van deze overeenkomst.

3.4 In afwijking van bepaling 3.2 is het Verwerker toegestaan om de persoonsgegevens te verwerken als een wettelijk voorschrift hem tot verwerking verplicht. In dat geval stelt de Verwerker, voorafgaand aan de verwerking, Verwerkingsverantwoordelijke in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

3.5 De maximale categorieën van persoonsgegevens die partijen verwachten te verwerken en de andere gegevens die Gebruikers wensen in te voeren in de software, zijn vastgelegd in bijlage 1.

4 GEHEIMHOUDING

4.1 Verwerker zal de persoonsgegevens tegenover derden geheimhouden en zal deze niet openbaar maken, anders dan voor zover noodzakelijk voor het verlenen van de Diensten dan wel voor zover een wettelijk voorschrift of rechterlijk bevel Verwerker tot mededeling c.q. verstrekking verplicht.

4.2 Verwerker staat er voor in en garandeert dat werknemers en alle overige natuurlijke personen die handelen onder zijn gezag en toegang hebben tot de persoonsgegevens eveneens onder dezelfde voorwaarden geheimhouding zullen betrachten ten aanzien van voornoemde informatie.

5 BEVEILIGINGSMAATREGELEN EN PERIODIEKE REVIEW DAARVAN

5.1 Verwerker zal technische- en organisatorische maatregelen nemen om de persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking, alsmede om een passende mate van betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) te waarborgen. Deze maatregelen zullen passend zijn, rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen.

5.2 Bij de beoordeling van een passend veiligheidsniveau zal Verwerker in het bijzonder aandacht schenken aan risico's die zich voordoen bij persoonsgegevensverwerking, zoals in het bijzonder de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot de doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

5.3 Verwerker zal in het kader van de in de vorige twee leden beschreven verplichtingen, tenminste de in Bijlage 2 gespecificeerde maatregelen treffen.

5.4 De door Verwerker in het kader van lid 1 en lid 2 te nemen maatregelen zullen in ieder geval voldoen aan de ISO27001 standaard. Verwerker zal op eerste verzoek van Verwerkingsverantwoordelijke een door een onafhankelijke en ter zake deskundige derde afgegeven certificaat overleggen ten bewijze hiervan. Het betreffende certificaat mag niet ouder zijn dan 12 maanden.

5.5 Verwerker zal periodiek de technische- en organisatorische maatregelen die genomen zijn om de verwerking te beveiligen testen, beoordelen en evalueren, al dan niet door inschakeling van een ter zake deskundige derde. Als uit deze beoordeling volgt dat de genomen maatregelen niet langer voldoende zijn, dan zal Verwerker alle redelijke stappen nemen om het beveiligingsniveau te verbeteren.

5.6 Verwerker zal al het noodzakelijke doen om te verzekeren dat enige natuurlijk persoon, die handelt onder het gezag van Verwerker en die toegang heeft tot persoonsgegevens deze gegevens niet zal verwerken tenzij op basis van instructies van Verwerkingsverantwoordelijke, of indien hij of zij daartoe verplicht wordt op grond van wetgeving.

5.7 Verwerker verleent Verwerkingsverantwoordelijke, tegen redelijke kosten, bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 t/m 36 van de Privacy Verordening.

6 INBREUK

6.1 Verwerker informeert Verwerkingsverantwoordelijke over iedere Inbreuk. Deze informatie wordt gegeven zonder onredelijke vertraging, doch in ieder geval binnen 24 uur, zodra hij daarvan kennis heeft genomen. In Bijlage 3 dienen aanspreekpunten en contactgegevens te worden vastgelegd.

6.2 In de, in het vorige lid bedoelde kennisgeving wordt ten minste het volgende omschreven of meegedeeld, voor zover Verwerker deze informatie heeft:

a.) De aard van de Inbreuk, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;

b.) De naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;

c.) De waarschijnlijke gevolgen van de Inbreuk;

d.) De maatregelen die Verwerker heeft voorgesteld of genomen om de Inbreuk aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan;

e.) Enige andere informatie die Verwerkingsverantwoordelijke nodig heeft op basis van de Toepasselijke Privacy Wetgeving.

6.3 Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.

6.4 Verwerker zal Verwerkingsverantwoordelijke ondersteunen bij het naleven van alle verplichtingen op basis van de Toepasselijke Privacy Wetgeving, rekening houdende met de aard van de verwerking en de informatie die beschikbaar is voor de verwerker. Deze ondersteuning houdt ook in het informeren van betrokkenen van een Inbreuk indien de Toepasselijke Privacy Wetgeving daartoe verplicht.

6.5 Verwerker documenteert alle Inbreuken, met inbegrip van de feiten omtrent de Inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen, alsmede alle andere relevante informatie omtrent de Inbreuk.

7 LOCATIE VAN GEGEVENS

7.1 Verwerker zal persoonsgegevens louter binnen de grenzen van de Europese Economische Ruimte (EER) verwerken (of doen verwerken), tenzij

a.) Het overdragen van persoonsgegeven naar buiten de EER door Verwerkingsverantwoordelijke wordt geautoriseerd of geïnstrueerd; of

b.) Wetgeving waar Verwerker aan is onderworpen, Verwerker verplicht tot overdracht naar buiten de EER. Indien Verwerker hiertoe verplicht wordt, zal Verwerker Verwerkingsverantwoordelijke terstond informeren, tenzij deze wetgeving Verwerker dit verbiedt.

8 SUB-VERWERKER

8.1 Verwerker zal geen Sub-Verwerker aanstellen, tenzij ze daartoe expliciet geautoriseerd wordt door Verwerkingsverantwoordelijke.

8.2 Verwerkingsverantwoordelijke autoriseert Verwerker hierbij om Proserve BV (Oostmaaslaan 71, 3063 AN Rotterdam) te betrekken als Sub-Verwerker.

8.3 Indien er een Sub-Verwerker wordt aangesteld, dan:

a.) Blijft Verwerker onverkort aansprakelijk voor de nakoming van de verplichtingen uit onderhavige overeenkomst;

b.) Zal Verwerker de aanstelling van een Sub-Verwerker in een schriftelijke overeenkomst vastleggen;

c.) Staat Verwerker er voor in dat alle verplichtingen die op grond van deze verwerkersovereenkomst rusten op Verwerker mede komen te rusten op deze Sub-Verwerker;

d.) Staat Verwerker er voor in dat de betreffende Sub-Verwerker ook de schriftelijke instructies van Verwerkingsverantwoordelijke opvolgt.

9 RECHTEN VAN BETROKKENEN

9.1 De Toepasselijke Privacy Wetgeving geeft de betrokkene bepaalde rechten. De verantwoordelijkheid voor het omgaan met (de uitvoering van) deze rechten rust bij Verwerkingsverantwoordelijke.

9.2 Verwerker zal, indien Verwerkingsverantwoordelijke daar om verzoekt, aan Verwerkingsverantwoordelijke alle noodzakelijke medewerking verlenen bij de nakoming van de verplichtingen van Verwerkingsverantwoordelijke verplichtingen op grond van de rechten genoemd in het vorige lid.

10 INFORMATIE, SAMENWERKING, CONTROLE EN NALEVING

10.1 Verwerker zal aan Verwerkingsverantwoordelijke alle informatie verstrekken met betrekking tot enige gedragscode of goedgekeurd certificeringsmechanisme waar zij aan gebonden is, zoals bedoeld in respectievelijk artikel 40 en artikel 42 van de Privacy verordening.

10.2 Op het eerste daartoe strekkende verzoek zal Verwerker aan Verwerkingsverantwoordelijke alle relevante informatie verstrekken betreffende de aspecten van de door hem verrichte verwerking van persoonsgegevens zodat Verwerkingsverantwoordelijke, mede aan de hand van die informatie, aan kan tonen dat zij de Toepasselijke Privacy Wetgeving naleeft.

10.3 Verwerkingsverantwoordelijke is gerechtigd om, middels een betrouwbare derde (gebonden aan geheimhouding), te controleren in hoeverre Verwerker de verplichtingen uit deze verwerkersovereenkomst naleeft. Verwerker zal aan een dergelijke controle kosteloos haar volledige medewerking verlenen.

10.4 De leden 2 en 3 zijn niet van toepassing voor zover een dergelijk verzoek of instructie:

- Een disproportionele last voor Verwerker met zich mee brengt;
- Niet is gerelateerd aan de verwerking van persoonsgegevens;
- Zou leiden tot het openbaren van bedrijfsgeheimen van Verwerker;
- Voor Verwerkingsverantwoordelijke niet zou leiden tot extra informatie bovenop de informatie die haar al is verstrekt in het kader van lid 1;
- In strijd zou zijn met wetgeving.

10.5 Indien een van de uitzonderingen uit het vorige lid zich voordoet zal Verwerker daar Verwerkingsverantwoordelijke onmiddellijk over informeren.

11 KOSTEN

11.1 De kosten voor de verwerking van gegevens die inherent zijn aan de normale uitvoering van de Diensten, worden geacht besloten te liggen in de Dienstverleningsovereenkomst(en) gespecificeerde (reeds verschuldigde) vergoeding(en) voor de Diensten.

11.2 Enige ondersteuning of enige andere aanvullende dienstverlening die Verwerker op grond van deze verwerkersovereenkomst dient te verlenen (bijv. op grond van artikel 6.4), of die wordt verzocht door Verwerkingsverantwoordelijke, inclusief alle verzoeken tot aanvullende informatie, zullen in rekening worden gebracht bij Verwerkingsverantwoordelijke overeenkomstig de in de Dienstverleningsovereenkomst(en) gespecificeerde tarieven. Voor betreffende werkzaamheden gelden de tarieven "Technische consultancy" zoals overeengekomen in de Dienstverleningsovereenkomst tussen Verwerkingsverantwoordelijke en Verwerker.

11.3 De voorgaande bepaling is niet van toepassing indien de werkzaamheden verband houden met een tekortkoming van Verwerker onder deze overeenkomst. De werkzaamheden zullen in dat geval kosteloos worden verricht (onverminderd het recht van Verwerkingsverantwoordelijke de daadwerkelijk geleden schade op Verwerker te verhalen). De bewijslast dat de betreffende tekortkoming niet toerekenbaar is ligt bij Verwerker.

12 AANSPRAKELIJKHEID

12.1 Enige beperking van de aansprakelijkheid in de Dienstverleningsovereenkomst(en) is *mutatis mutandis* ook van toepassing op deze verwerkersovereenkomst.

12.2 Indien en voor zover in de Dienstverleningsovereenkomst de aansprakelijkheid voor onrechtmatige verwerking van persoonsgegevens geheel is uitgesloten, is deze beperking – in afwijking van het vorige lid – niet van toepassing.

12.3 Indien er als gevolg van een toerekenbare tekortkoming van Verwerker, of een aan Verwerker toerekenbaar gedragen of nalaten, door een overheidstoezichthouder aan Verwerkingsverantwoordelijke een boete wordt opgelegd, welke boete (deels) rechtstreeks verband houdt met voornoemde tekortkoming, gedragen of nalaten, vrijwaart Verwerker Verwerkingsverantwoordelijke voor (dat deel van) die boete. De vrijwaring geldt niet voor zover de boete (mede) verband houdt met gedrag van Verwerkingsverantwoordelijke zelf.

12.4 Iedere beperking van aansprakelijkheid komt voorts te vervallen in geval van opzet of grove schuld aan de zijde van Verwerker.

13 GEVOLGEN VAN DE TOEPASSELIJKE PRIVACY WETGEVING

13.1 Verwerker garandeert dat de Diensten gebruikt kunnen worden in overeenstemming met de Toepasselijke Privacy Wetgeving. Deze garantie geldt alleen voor de Toepasselijke Privacy Wetgeving in de landen die zijn beschreven in Bijlage 1, bij gebreke waarvan het land van vestiging van Verwerkingsverantwoordelijke gelezen wordt. Verwerker heeft geen kennis van andere Aanvullende Nationale Wetgeving of Implementatiewetgeving.

13.2 Verwerkingsverantwoordelijke moet Verwerker informeren over enige Aanvullende Nationale Wetgeving of Implementatiewetgeving, voor zover van belang voor de uitvoering van de Diensten, indien Verwerkingsverantwoordelijke wil dat Verwerker ook persoonsgegevens verwerkt met betrekking tot de activiteiten van Verwerkingsverantwoordelijke in andere landen van de EU, niet zijnde de landen vermeld in Bijlage 1.

13.3 Verwerker zal Verwerkingsverantwoordelijke informeren indien zij, op basis van de informatie door Verwerkingsverantwoordelijke verstrekt in overeenstemming met het vorige lid, vermoedt dat het uitvoeren van de Diensten (gedeeltelijk) in strijd is met enige Aanvullende Nationale Wetgeving of Implementatiewetgeving.

14 DUUR, BEËINDIGING EN GEVOLGEN VAN BEËINDIGING

14.1 De duur van deze verwerkersovereenkomst is gelijk aan de duur van de Dienstverleningsovereenkomst(en).

14.2 Deze verwerkersovereenkomst wordt automatisch beëindigd indien alle Dienstverleningsovereenkomsten zijn beëindigd.

14.3 Verplichtingen welke naar hun aard bestemd zijn om ook na beëindiging of ontbinding van de verwerkersovereenkomst voort te duren, blijven na beëindiging c.q. ontbinding van deze verwerkersovereenkomst bestaan. Tot deze verplichtingen behoren onder meer:

a.) Vrijwaring voor boetes van toezichthouders;
b.) Geheimhouding;
c.) Geschillenbeslechting, toepasselijk recht.

14.4 In het geval dat een Dienstverleningsovereenkomst is beëindigd zal Verwerker, ter vrije keuze van Verwerkingsverantwoordelijke, de in het kader van de Diensten verwerkte persoonsgegevens vernietigen of terug leveren.

14.5 Verwerker zal, hangende de keuze van Verwerkingsverantwoordelijke om de verwerkte persoonsgegevens te vernietigen, de persoonsgegevens blijven bewaren. Verwerker is niet gerechtigd de persoonsgegevens zonder uitdrukkelijke instructie daartoe van Verwerkersverantwoordelijke te vernietigen. Verwerker zal alle bestanden en data van Verwerkersverantwoordelijke maximaal 60 dagen nadat de overeenkomst is beëindigd als gevolg van opzegging of ontbinding opslaan en beschikbaar houden zodat Verwerkersverantwoordelijke (of de door Verwerkersverantwoordelijke aangewezen Derde) zijn bestanden en data kan opvragen of vernietigen. Na ommekomst van die termijn zal Verwerker de bestanden en data verwijderen tenzij Verwerkersverantwoordelijke de Verwerker Schriftelijk verzoekt om de bestanden en data gedurende een alsdan nader door Opdrachtgever te bepalen aanvullende termijn te bewaren, alvorens het vernietigd wordt.

14.6 Het terug leveren van de persoonsgegevens geschiedt in een algemeen leesbaar en deugdelijk gedocumenteerd bestandsformaat.

14.7 Ongeacht het voorgaande:

a.) Is Verwerker gerechtigd om de gegevens te bewaren indien wetgeving haar daartoe verplicht.

b.) Zal Verwerker informatie met betrekking tot Inbreuken, zoals bedoeld in artikel 6.5, tenminste tot een jaar na beëindiging van de Dienstverleningsovereenkomst(en) bewaren.

15 OVERIGE BEPALINGEN

15.1 Voor zover enige bepaling van deze verwerkersovereenkomst in strijd is met hetgeen in de Dienstverleningsovereenkomst(en) is bepaald, prevaleert hetgeen in deze verwerkersovereenkomst is bepaald (voor zover de strijdigheid betrekking heeft op het verwerken van persoonsgegevens).

15.2 Voor alle onderwerpen die niet in deze verwerkersovereenkomst zijn geregeld geldt dat de bepalingen van de relevante Dienstverleningsovereenkomst *mutatis mutandis* van toepassing zijn op de verwerking van persoonsgegevens in het kader van die specifieke Dienst.

15.3 Wijzigingen op deze verwerkersovereenkomst en/of de bijlagen zijn alleen geldig voor zover deze schriftelijk zijn vastgelegd en zijn ondertekend door beide partijen.

15.4 Deze verwerkersovereenkomst kan (gedeeltelijk) worden vervangen door standaard contractsbepalingen als bedoeld in artikel 28 lid 6 van de Privacy verordening, indien zulke bepalingen voor beide partijen wederzijds acceptabel zijn

16 TOEPASSELIJK RECHT EN BEVOEGDE RECHTER

16.1 Op deze overeenkomst is Nederlands recht van toepassing. Behoudens voor zover de overeenkomst(en) met betrekking tot de Diensten een exclusief bevoegde rechter aanwijzen, is de rechter gevestigd in het arrondissement waar Verwerkingsverantwoordelijke vestigingsplaats heeft exclusief bevoegd.

1. VERWERKING GEGEVENS

1.1 Soorten gegevens

Gegevens die zullen worden verwerkt in het kader van de Overeenkomst van Opdracht:

- ✓ Van medewerkers:
  - Nummer en/of naam
- ✓ Van productiegegevens:
  - Werkordernummer, afdelingscode, bewerkingsstappen, artikelen, voorraadgegevens, picklijsten, magazijnlocaties.

1.2 De doeleinden van de verwerking van gegevens

- ✓ Van medewerkers:
  - Via de naam of nummer van de medewerker uit ERP worden de gewerkte uren teruggekoppeld naar ERP.
- ✓ Van productiegegevens:
  - Werkorders en de daaraan gekoppelde artikelen worden opgehaald uit ERP in verwerkt in de Smart Production Suite. De verwerking houdt in dat een orderstatus wordt aangepast in ERP en de daarbij behorende transacties zoals voorraadhoogtes en verbruikte materialen en uren.

1.3 Aard van de verwerking van gegevens

Gegevens komen via automatische gegevensuitwisseling met ERP systeem:

- ✓ Ontvangst op SFTP-server of via webservices Smart Production Solutions
- ✓ Verwerking gegevens in database Smart Production Suite en dan weer teruggekoppeld naar ERP
- ✓ Opschoning/ vernietiging gebeurt op basis van opdrachten van klant.

1.4 Landen waarop deze diensten gericht zijn

De diensten zijn gericht op Nederland.

2. TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

2.1 Inbedding informatiebeveiliging in de organisatie

Binnen het personeelsmanagement is expliciet aandacht voor:

- ✓ Awareness op het gebied van informatiebeveiliging; Er wordt meerdere keren per jaar een kennisavond gehouden over het belang van informatiebeveiliging voor onze klanten en het voortbestaan van ons bedrijf. Tevens worden periodiek posters en andere visuele ondersteuning gebruikt om mensen op procedures te wijzen (bij de papierbak een lijst welke spullen wel en welke niet in die papierbak mogen, idem bij de printer omtrent wat geprint mag worden, etc.). Hierbij worden naast procedures ook potentiële gevolgen van verkeerd handelen voor de personen waarover informatie in onze systemen vastligt getoond. Dit heeft als doel de medewerkers niet alleen te motiveren om puur de procedures te volgen maar ook om altijd zelf kritisch te blijven nadenken of er niet zaken worden gedaan die voor onze klanten grote nadelige gevolgen kunnen hebben. Ook in het personeelshandboek zijn diverse richtlijnen rondom informatiebeveiliging opgenomen en wordt actief gewezen op het informatiebeveiligingsbeleid.
- ✓ Competenties; Er wordt zowel actief beoordeeld (bij indiensttreding en daarna elk jaar) of de competenties van de medewerker goed aansluiten bij de functie die hij heeft of dat hier ontwikkeling op nodig is (danwel wijziging van de functie). Tevens wordt bij personele wijzigingen actief beoordeeld of de juiste competenties nog in het bedrijf aanwezig zijn of dat er gaten ontstaan (waarvoor dan een maatregel genomen moet worden).
- ✓ Integriteit; Bij de aanname van medewerkers worden een aantal acties uitgevoerd om vast te stellen of de persoon integer is voor het werken met privacy gevoelige gegevens:
- ✓ Diploma/referentiecheck
- ✓ VOG aanvragen
- ✓ Ondertekenen geheimhoudingsverklaring
- ✓ Voor medewerkers die in contact komen met klantgegevens worden door verscheidene klanten aanvullende persoonlijke screenings uitgevoerd.
- ✓ Actieve beoordeling op werken in lijn met informatiebeveiligingsbeleid; in de beoordelings-gesprekken wordt actief stilgestaan bij in hoeverre de persoon goed handelt naar de richtlijnen en eisen in ons informatiebeveiligingsbeleid. Indien een medewerker hier niet goed op acteert worden actief waarschuwingen gegeven die kunnen resulteren in beëindiging van de dienstbetrekking. Om te voorkomen dat er een angstcultuur ontstaat geldt dat het zelf melden van zelf veroorzaakte incidenten veel minder negatief wordt beoordeeld dan het niet zelf melden.

2.2 Logische en fysieke toegangsbeveiliging

De belangrijkste maatregel op dit vlak is het feit dat de kantoor-omgeving (zonder klantgegevens m.u.v. financiële administratie) en productie-omgeving (met klantgegevens) strikt fysiek en logisch gescheiden zijn. Hierdoor geldt:

1. Geen enkele medewerker van Smart Production Solutions heeft fysiek zelfstandig toegang tot de ruimtes waar de klantgegevens staan. Hiervoor is altijd medewerking van de hostingpartner (Proserve) noodzakelijk en goedkeuring van de directie.
2. Toegang (fysiek en logisch) wordt voor elke medewerker verleend na beoordeling door de directie.
3. In het indiensttredings- en uitdiensttredingsprotocol is een checklist opgenomen waarmee wordt gecontroleerd of alle fysieke en logische toegang is afgesloten (alsmede een aantal andere stappen op het gebied van inleveren van apparatuur etc.).
4. De logische toegang tot de productie-omgeving is apart afgeschermd:
    a. Er is voor een beperkte set medewerkers toegang tot deze omgeving (alleen indien noodzakelijk voor uitoefening functie)
    b. Deze krijgen een aparte gebruikersnaam en wachtwoord, geïnstalleerd certificaat en tweede factor (time-based token) om contact te maken (VPN) met de productie-omgeving. Tevens is toegang tot dit VPN netwerk alleen mogelijk vanaf de IP-range van kantoor.
    c. Vervolgens kan deze medewerker met een andere gebruikersnaam en wachtwoord daadwerkelijk op verschillende servers inloggen. Toegang tot de servers is hier beperkt op basis van de functie. Alleen de echt noodzakelijke servers zijn toegankelijk.
    d. Ook deze toegangsrechten worden actief bijgewerkt bij functiewijzigingen en uitdiensttreding en worden nog jaarlijks door de directie gecontroleerd op juistheid.

2.3 Functioneel beheer, verbinding en hosting

Binnen de Smart Production Suite zelf kunnen klantbeheerders zelf rollen toekennen aan gebruikers. Op basis van deze rollen wordt bepaald door de software welke wijzigingen gebruikers wel en welke ze niet mogen doen. Basis van deze autorisatie is dat de rol bepaalt wat een gebruiker mag doen en dat de koppeling aan operational groups van de individuele gebruiker bepaalt voor welke set jobs een gebruiker dat mag doen.

Tezamen bepalen ze of een bepaalde wijziging wel of niet wordt toegestaan. Hierbij geldt uiteraard dat de binnenkomende requests serverside hierop beoordeeld worden.

Voor het beheer van de servers waarop de software (en klantgegevens) staan geldt dat een medewerker ook een in de Active Directory gedefinieerde rol krijgt toegewezen. Deze rol-toewijzing wordt bijgehouden en nog periodiek gecontroleerd op juistheid.

Vervolgens wordt het standaard windows-mechanisme gebruikt voor beperking van rechten.

Voor toegang tot deze beheeromgeving moet een VPN-verbinding worden gelegd die een IP-filtering kent (alleen toegang vanuit kantoor Smart Production Solutions en een back-up-locatie) alsmede 2FA.

Als aanvullende maatregel heeft Smart Production Solutions een SIEM ingericht die zowel het dataverkeer als de logging van uitgevoerde acties verzamelt en analyseert. Hiermee kan aanvullend worden beoordeeld (en actief geëscaleerd) indien een gebruiker of softwarecomponent ‘ongewone’ acties doet.

Al het verkeer naar de productie-omgeving komt via een fysieke firewall binnen, waarbij alleen verkeer wordt toegestaan dat expliciet wordt opengezet (en dus is goedgekeurd in via de change-procedures). Vervolgens

wordt het verkeer gerouteerd over een gesegmenteerd netwerk waarbij alleen servers die daarvoor bedoeld zijn, bereikbaar zijn via internet (de web- en koppeling servers).

Webverkeer is altijd beveiligd via SSL, waarbij de SSL-instellingen via externe tools getoetst worden op bekende kwetsbaarheden. Bestandsuitwisseling verloopt of via VPN of via SFTP.

De databaseservers zijn niet rechtstreeks door het webverkeer te benaderen en kennen gescheiden databases per klant.

2.4 Monitoring en verbetering beveiligingsmaatregelen & -incidenten

Als een non-conformiteit wordt vastgesteld dan wordt een plan van aanpak vastgesteld waarmee deze non-conformiteit kan worden opgeheven en of er aanvullende maatregelen noodzakelijk zijn om te voorkomen dat deze non-conformiteit herhaaldelijk optreedt. Ook kan het zijn dat gekozen werkwijzes dusdanig suboptimaal zijn dat de verleiding om ze te omzeilen te groot is.

Om te monitoren of genomen maatregelen het gewenste effect hebben wordt bij elke maatregel expliciet vastgesteld op welke manier en hoe vaak de effectiviteit gemeten wordt. De verantwoordelijke contactpersonen voeren dit vervolgens uit. Tijdens de audit wordt gecontroleerd voor alle controls of dit wel is gedaan.

Beveiligingsincidenten worden in de periodieke awareness-sessies en, indien door een individu danwel afdeling veroorzaakt, met de betrokken medewerkers van Smart Production Solutions besproken. Indien een beveiligingsincident leidt tot een (potentieel) datalek, wordt de procedure ‘Meldplicht Datalekken’ gevolgd, waarbij binnen 24 uur de betrokken Verantwoordelijke(n) worden geïnformeerd conform de richtlijnen van de Autoriteit Persoonsgegevens

2.5 Softwareontwikkeling

Smart Production Solutions heeft Secure Development principes in haar ontwikkelmethodiek opgenomen. Bij elke individuele wijziging wordt beoordeeld wat de impact op het gebied van beveiliging is. Hierbij heeft Smart Production Solutions voor haar developers een checklist beschikbaar die is opgesteld op basis van de OWASP-top 10 richtlijnen, ISO27002 controls, NCSC en NIST.

Competenties van ontwikkelaars worden met behulp van internen en externen ontwikkeld en up-to-date gehouden op het gebied van secure programming.

2.6 Back-up & restore procedures

Data wordt tegen vernietiging beschermd middels een back-upproces dat 7 dag-, 3 week-, 11 maand- en jaarback-ups van specifieke klantdatabases geëncrypt op een andere locatie bewaart.

Tevens worden back-ups periodiek getoetst door middel van restores.

Daarnaast heeft Smart Production Solutions permanent een back-up-locatie ingericht waarmee de applicatie weer binnen de in de SLA afgesproken periode up-and-running kan worden gebracht, mocht de primaire locatie vernietigd worden.

BIJLAGE 3 BIJ VERWERKERSOVEREENKOMST

CONTACTGEGEVENS

Hier invoegen contactgegevens medewerker VERWERKERSVERANTWOORDELIJKE waarmee contact dient te worden opgenomen in het geval van "incidenten"/datalekken.

Primaire melding:
Supportdesk Smart Production Solutions
support@smartproductionsolutions.nl
073-6159950

Daarnaast dient de functionaris voor de gegevensbescherming (FG) en/of de information security officer (ISO) geïnformeerd te worden.

Primair aanspreekpunt Verwerkersverantwoordelijke:

FG dan wel ISO	
**Naam*	
**Email*	
**Telefoon*	
**Mobiel*	

Bij afwezigheid:

FG dan wel ISO	
**Naam*	
**Email*	
**Telefoon*	
**Mobiel*	

** Graag digitaal dan wel schriftelijk aan te vullen door Verwerkersverantwoordelijke*

Primair aanspreekpunt Verwerker:

FG
privacy@othersidesoftware.com
073 615 9950 (kantoortijden)

Bij afwezigheid:

Director
Eric Klement
eric.klement@smartproductionsolutions.nl
073 615 9950 (kantoortijden)
06-57837958