Verwerkersovereenkomst T.S.D. The Software Desk B.V. (Planning.nl)

Deze Verwerkersovereenkomst is van toepassing op alle vormen van verwerking van persoonsgegevens die T.S.D. The Software Desk B.V., ingeschreven bij de Kamer van Koophandel onder nummer 24292101, (hierna: Verwerker) uitvoert ten behoeve van een wederpartij aan wie zij diensten levert (hierna: Verantwoordelijke).

1. Doeleinden van verwerking

1.1. Verwerker verbindt zich onder de voorwaarden van deze Verwerkersovereenkomst in opdracht van Verantwoordelijke persoonsgegevens te verwerken overeenkomstig Appendix 1. Verwerking zal uitsluitend plaatsvinden in het kader van het in de 'private cloud' van Verwerker opslaan van gegevens van Verantwoordelijke, en bijbehorende online diensten, ten behoeve van projectplanning, projectbeheer en/of planning van resources van Verantwoordelijke, plus die doeleinden die daarmee redelijkerwijs samenhangen of die met nadere instemming worden bepaald.

1.2. Verwerker zal de persoonsgegevens niet voor enig ander doel verwerken dan zoals door Verantwoordelijke is vastgesteld. Verantwoordelijke zal Verwerker op de hoogte stellen van de verwerkingsdoeleinden voor zover deze niet reeds in deze Verwerkersovereenkomst zijn genoemd.

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

1.4. Verantwoordelijke staat ervoor in dat de verwerking van persoonsgegevens wordt geregistreerd volgens artikel 30 van de AVG.

1.5. Verantwoordelijke maakt voor het administreren van de persoonsgegevens in het kader van projectplanning, projectbeheer en/of planning van resources van Verantwoordelijke gebruik van de door Verwerker ontwikkelde en onderhouden online planningsapplicaties. Verwerker is niet degene die de persoonsgegevens daadwerkelijk invoert, wijzigt en verwerkt, dat is strikt voorbehouden aan Verantwoordelijke. Verwerker fungeert ter zake van dit systeem als Support en Service Desk met betrekking tot de online planningsapplicaties. Verwerker garandeert dat Verwerker geen andere verwerkingshandelingen zal uitvoeren ten aanzien van de persoonsgegevens van Verantwoordelijke dan in het kader van Support en Service Desk-werkzaamheden. Verwerker verwerkt de persoonsgegevens te allen tijde op behoorlijke en zorgvuldige wijze in overeenstemming met de toepasselijke wet- en regelgeving, de (specifieke) instructies en aanwijzingen van Verantwoordelijke.

2. Verplichtingen Verwerker

2.1. Ten aanzien van de in artikel 1 genoemde verwerkingen zal Verwerker zorgdragen 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 AVG.

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

2.3. 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. Doorgifte van persoonsgegevens

3.1. De Verwerker mag de persoonsgegevens uitsluitend verwerken in Nederland. Doorgifte naar andere landen is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van Verantwoordelijke en met inachtneming van de toepasselijke wet- en regelgeving.

4. Verdeling van verantwoordelijkheid

4.1. Verwerker stelt ten behoeve van de verwerkingen ICT-diensten ter beschikking die door Verantwoordelijke te gebruiken zijn voor de hierboven genoemde doelen. Verwerker verricht zelf alleen op basis van aparte afspraken verwerkingen.

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

4.3. Verantwoordelijke garandeert dat de inhoud, het gebruik en de opdracht tot de verwerkingen van de persoonsgegevens zoals bedoeld in deze Overeenkomst, niet onrechtmatig is en geen inbreuk maken op enig recht van derden.

5. Inschakelen derden en subverwerkers

5.1. Verwerker maakt in het kader van de Verwerkersovereenkomst gebruik van de diensten van SmartDC voor opslag van data. De contactgegevens van de subverwerker zijn gegeven in appendix 2.

5.2. Verwerker zal haar activiteiten die (deels) bestaan uit het verwerken van de Persoonsgegevens of vereisen dat Persoonsgegevens verwerkt worden niet uitbesteden aan een andere derde partij zonder voorafgaande, schriftelijke toestemming van Verantwoordelijke (Toestemming als bijlage aanhechten)

5.3. Verwerker zorgt er onvoorwaardelijk voor dat deze derden schriftelijk dezelfde plichten op zich nemen als tussen Verantwoordelijke en Verwerker is overeengekomen. Verwerker staat in voor een correcte naleving van deze plichten door deze derden en is bij fouten van deze derden zelf jegens Verantwoordelijke aansprakelijk voor alle schade alsof hij zelf de fout(en) heeft begaan.

6. Beveiliging

6.1. Verwerker zal zich inspannen voldoende technische en organisatorische maatregelen te nemen 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). Gedetailleerd inzicht in onze beveiligingsmaatregelen maakt Verwerker - om veiligheidsredenen - niet openbaar. De maatregelen zijn beschreven in het ISMS van Planning.nl, dat op kantoor van Planning.nl kan worden ingezien. De verklaring van toepasselijkheid bij het ISMS en de ISO-27001 certificering is gegeven is Appendix 3. Een overzicht van de minimale maatregelen die Verwerker moet treffen zijn beschreven in Appendix 4.

6.2. Verwerken zal ervoor zorgdragen dat het beveiligingsniveau is afgestemd op de risico's, rekening houdend met de stand van de techniek en de kosten van de beveiligingsmaatregelen.

6.3. Planning.nl is ISO 27001 gecertificeerd en wordt met de volgens deze norm vereiste regelmaat geaudit.

7. Meldplicht

7.1. Verantwoordelijke is te allen tijde verantwoordelijk voor het melden van een beveiligingslek en/of datalek (waaronder wordt verstaan: een inbreuk op de beveiliging van persoonsgegevens die leidt tot een kans op nadelige gevolgen, dan wel nadelige gevolgen heeft, voor de bescherming van persoonsgegevens) aan de toezichthouder en/of betrokkenen. Om Verantwoordelijke in staat te stellen aan deze wettelijke plicht te voldoen, stelt Verwerker de Verantwoordelijke binnen 24 uur nadat het lek bij hem bekend is geworden op de hoogte van het beveiligingslek en/of het datalek.

7.2. Een melding moet altijd worden gedaan, maar alleen als de gebeurtenis zich daadwerkelijk voorgedaan heeft.

7.3. Verwerker meldt het datalek telefonisch/per email via Edwin Thier of via de Security Officer van Planning.nl.

7.4. De meldplicht behelst in ieder geval het melden van het feit dat er een lek is geweest. Daarnaast behelst de meldplicht:

- contactgegevens voor de opvolging van de melding
- wie geïnformeerd is (zoals de betrokkene zelf, Verantwoordelijke, toezichthouder)
- de aard van het datalek;
- de (vermeende) oorzaak van het datalek;
- waar mogelijk de categorieën en, bij benadering, het aantal van betrokkenen en Persoonsgegevens die zijn getroffen door het datalek;
- de reeds bekende en te verwachten gevolgen van het Datalek;
- de maatregelen die de Verwerker heeft getroffen en zal treffen om de gevolgen van het datalek (zo veel mogelijk) te beperken;

7.5. Wanneer een beveiligingslek of datalek optreedt

- zal Verwerker alle redelijke maatregelen nemen om (verdere) schending van de AVG te voorkomen en/of beperken. Daarbij zal Verwerker zich waar mogelijk onthouden van het nemen van maatregelen die onomkeerbaar zijn en/of een onderzoek naar de oorzaken van het beveiligings- of datalek ernstig belemmeren.

- zal Verwerker haar medewerking verlenen aan Verantwoordelijke en Verantwoordelijke ondersteunen in het uitvoeren van haar wettelijke verplichtingen ten aanzien van het geconstateerde incident.
- zal Verwerker Verantwoordelijke ondersteunen bij de op Verantwoordelijke rustende meldplicht ten aanzien van de inbreuk in verband met persoonsgegevens bij de Autoriteit Persoonsgegevens en/of betrokkene, zoals bedoeld in artikel 33 lid 3 en artikel 34 lid 1 van de AVG.

8. Afhandeling verzoeken van betrokkenen

8.1. In het geval dat een betrokkene een verzoek tot inzage, zoals bedoeld in de AVG artikel 15, rectificatie, volgens artikel 16, gegevenswissing, volgens artikel 17, of beperking van de verwerking, volgens artikel 18, richt aan Verwerker, zal Verwerker de betrokkene doorverwijzen naar Verantwoordelijke. Verwerker zal zover redelijkerwijs (volgens SLA) mogelijk ondersteuning bieden aan Verantwoordelijke om binnen de wettelijke termijnen te voldoen aan de deze en andere verplichtingen jegens betrokkenen op grond van de AVG, als dit bij de uitvoering van de verzoeken nodig mocht zijn. Dit eerst nadat door Verwerker is vastgesteld, dat de aanvrager voor deze ondersteuning geautoriseerd is om deze aanvraag te doen.

8.2. Verwerker ondersteunt Verantwoordelijke om specifieke verplichtingen vanuit de AVG na te komen, zoals uitvoering Data Protection Impact Assessment (DPIA), als dit noodzakelijk is voor de betreffende verwerking.

8.3. Verwerker zet zich op verzoek van Verantwoordelijke naar vermogen in om mee te werken aan het bieden van ontwerp infrastructuur, software, inrichting van software en interfaces die het beschermen van persoonsgegevens afdwingen of makkelijk toepasbaar maken (privacy by design en privacy by default).

8.4. Wanneer werkzaamheden binnen de scope van het afgesloten contract met Planning.nl vallen zijn hier geen kosten aan verbonden. Eventuele extra kosten die buiten het contract vallen kunnen worden doorbelast aan Verantwoordelijke.

9. Geheimhouding en vertrouwelijkheid

9.1. Op alle persoonsgegevens die Verwerker van Verantwoordelijke 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. Verwerker screent alle medewerkers voorafgaand aan het dienstverband en laat elke medewerker als onderdeel van de arbeidsovereenkomst een geheimhoudingsclausule tekenen, waarin onder andere geheimhouding ten aanzien van persoonsgegevens is opgenomen.

9.3. Verwerker neemt alle mogelijke maatregelen om te zorgen dat geheimhouding wordt nagekomen. Maatregelen zijn opgenomen in het ISMS en zijn zo een onderdeel van de audits t.b.v. de ISO 27001 certificering.

9.4. Deze geheimhoudingsplicht is niet van toepassing voor zover Verantwoordelijke 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.

9.5. Indien Verwerker op grond van een wettelijke verplichting gegevens dient te verstrekken, zal Verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal Verwerker de Verwerkingsverantwoordelijke zo spoedig mogelijk ter zake informeren. Tenzij wettelijke bepalingen dit verbieden.

10. Audit

10.1. Verantwoordelijke heeft het recht om audits uit te laten voeren door een onafhankelijke ICT-deskundige die aan geheimhouding is gebonden ter controle van naleving van alle punten uit de Verwerkersovereenkomst.

10.2. Deze audit mag eens per jaar plaatsvinden.

10.3. Verwerker zal aan de audit meewerken en alle voor de audit redelijkerwijs relevante informatie, inclusief ondersteunende gegevens zoals systeemlogs, en medewerkers zo tijdig mogelijk ter beschikking stellen.

10.4. De bevindingen naar aanleiding van de uitgevoerde audit zullen door Partijen in onderling overleg worden beoordeeld en, naar aanleiding daarvan, al dan niet worden doorgevoerd door één van de Partijen of door beide Partijen gezamenlijk.

10.5. Kosten worden door Verantwoordelijke gedragen tenzij de audit uitwijst dat Verwerker haar processen niet voldoende ingeregeld heeft volgens de wettelijke eisen van de AVG.

11. Aansprakelijkheid

11.1. Verwerker is slechts aansprakelijk voor de schade die door verwerking is veroorzaakt wanneer bij de verwerking niet is voldaan aan de specifiek tot verwerkers gerichte verplichtingen van de AVG of andere toepasselijke regelgeving betreffende de verwerking van Persoonsgegevens of buiten dan wel in strijd met de rechtmatige instructies van de Verantwoordelijke is gehandeld en slechts voor zover en tot het bedrag dat de schade aan Verwerker of een door haar ingeschakelde derde kan worden toegerekend.

11.2. De aansprakelijkheid van Verwerker voor schade als gevolg van een toerekenbare tekortkoming in de nakoming van de Verwerkersovereenkomst, dan wel uit onrechtmatige daad of anderszins, is -buiten gevallen waar de wet anders voorschrijft- per gebeurtenis (een reeks opeenvolgende gebeurtenissen geldt als één gebeurtenis) beperkt tot de vergoeding van directe schade, tot maximaal het bedrag van de door de verzekeraar van Planning.nl gedane uitkering.
In het geval dat de verzekeraar niet uitbetaalt, is de vergoeding beperkt tot maximaal het bedrag van de door Verwerker ontvangen vergoedingen voor de werkzaamheden onder deze Verwerkersovereenkomst over de maand voorafgaande aan de schadeveroorzakende gebeurtenis. De aansprakelijkheid van Verwerker voor directe schade zal in het laatste geval totaal nooit meer bedragen dan EUR 15.000,-

11.3. Verwerker dient adequaat verzekerd te zijn en te blijven tegen aanspraken van de Verantwoordelijke.

11.4. Onder directe schade wordt uitsluitend verstaan alle schade bestaande uit:

- schade direct toegebracht aan stoffelijke zaken (“zaakschade”)
- redelijke en aantoonbare kosten om Verwerker ertoe te manen de Verwerkersovereenkomst (weer) deugdelijk na te komen
- 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

12. Duur en beëindiging

12.1. Deze Verwerkersovereenkomst komt tot stand door ondertekening van Partijen en op de datum van de laatste ondertekening.

12.2. Deze Verwerkersovereenkomst is aangegaan voor de duur zoals bepaald in de hoofdovereenkomst (dienstverleningsovereenkomst) tussen Partijen en bij gebreke daarvan in ieder geval voor de duur van de samenwerking tussen Partijen.

12.3. Zodra de Verwerkersovereenkomst, om welke reden en op welke wijze dan ook, is beëindigd, zal Verwerker op eerste verzoek van Verantwoordelijke alle persoonsgegevens die bij haar aanwezig zijn en eventuele kopieën daarvan verwijderen en/of vernietigen, tenzij Verwerker wettelijk verplicht is de persoonsgegevens op te slaan.

12.4. Verwerker is gerechtigd deze overeenkomst van tijd tot tijd te herzien. Zij zal minimaal drie maanden van tevoren mededeling doen van de wijzigingen aan Verantwoordelijke. Verantwoordelijke mag opzeggen tegen het einde van deze drie maanden indien zij niet akkoord kan gaan met de wijzigingen.

13. Toepasselijk recht en geschillenbeslechting

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

13.2. Alle geschillen, welke tussen Partijen mochten ontstaan in verband met de Verwerkersovereenkomst, zullen worden voorgelegd aan de bevoegde rechter voor het arrondissement waarin Verwerker gevestigd is.

14. Ondertekening

Door ondertekening van deze overeenkomst gaat u akkoord met de inhoud van deze overeenkomst. U verklaart bevoegd te zijn om deze overeenkomst met Planning.nl aan te gaan.

_____	**T.S.D. The Software Desk B.V.**
Klantnaam	
_____/_____/_____	…/…/20…
Datum	*Datum*
_____	E.S.C. Thier
Naam	*Naam*
_____	directeur
Functie	*Functie*
	
_____	_____
Handtekening	*Handtekening*

Appendix 1: Verwerking van Persoonsgegevens

1. Aard en doel van de Verwerking van de Persoonsgegevens

Plannen van resources

2. Categorieën van Verwerkingen van Persoonsgegevens die door Verwerker worden uitgevoerd

Technisch, applicatie- en databasebeheer van de productie-omgeving en ondersteunende diensten voor Visibox of Cloudplan. Het beheer bestaat uit:

- technisch beheer van de fysieke, virtuele servers en switches in de productieomgeving (datacenter)
- technisch beheer van de standaard software en besturingssystemen in de productieomgeving (datacenter)
- technisch beheer van de werkstations inclusief netwerkapparatuur
- applicatiebeheer van Visibox of Cloudplan
- databasebeheer van Visibox of Cloudplan

3. Overzicht van Verwerkingen van Persoonsgegevens die door subverwerkers worden uitgevoerd

Subverwerker: SmartDC Rotterdam (Van Nelleweg 1, 3044 BC Rotterdam) en SmartDC Heerlen (Kloosterweg 1, 6412 CN Heerlen).
SmartDC is ook ISO 27001 gecertificeerd.
De servers waarop verwerking van persoonsgegevens plaatsvindt zijn eigendom van Planning.nl staan bij SmartDC in een alleen voor Planning.nl toegankelijke ruimte. Alle data die door gebruikers (medewerkers van Verantwoordelijke) wordt opgeslagen, wordt opgeslagen in de voor Verantwoordelijke aangewezen database container op deze server.
SmartDC verwerkt zelf geen persoonsgegevens van klanten van Planning.nl.
Smart DC is verantwoordelijk voor beveiliging van de toegang, stroomvoorziening etc.

4. Categorieën van personen (Betrokkenen) van wie de Persoonsgegevens worden verwerkt

Persoonsgegevens hebben betrekking op personeelsleden van Verantwoordelijke.

5. Soort Persoonsgegevens dat wordt verwerkt

Dat kan afhankelijk van de wensen van Verantwoordelijke bijvoorbeeld zijn: naam, telefoonnummer, email adres, datum in dienst etc. Planning.nl adviseert om alleen gegevens in te voeren die nodig zijn voor het inplannen van de resources. Planning.nl en Verwerkingsverantwoordelijke zullen geen bijzondere persoonsgegevens in het systeem opslaan.

6. Bewaartermijn

De bewaartermijn van alle door Verantwoordelijke opgeslagen gegevens eindigt een maand na het beëindigen van het contract, tenzij Verwerker en Verantwoordelijke anders overeenkomen, of de wet anders voorschrijft. Twee weken na het verstrijken van deze bewaartermijn worden ook de back-ups verwijderd en worden alle gegevens definitief gewist.

Appendix 2: Contactgegevens Subverwerker

SmartDC Rotterdam

Van Nelleweg 1

3044 BC

Rotterdam

https://www.smartdc.net/nl/rotterdam/

SmartDC Heerlen

Kloosterweg 1

6412 CN

Heerlen

https://www.smartdc.net/nl/heerlen/

Appendix 3: Verklaring van toepasselijkheid t.b.v. ISO-27001 certificering

Maatregel	Omschrijving
BUITEN SCOPE	Niet van toepassing bij Planning.nl
IN SCOPE	

Hoofdstuk (ISO27001:2013)	Scope	Reden voor uitsluiting	Reden voor insluiting		
			volgens Risicobeheer aan de hand van MAPGOOD versie 2017	wet- en regel geving	gezonde bedrijfs voering
5 Informatie beveiligings-beleid	IN SCOPE				
5.1 Aansturing door de directie van de informatie-beveiliging	IN SCOPE				
5.1.1 Beleidsregels voor informatiebeveiliging	IN SCOPE		✓		
5.1.2 Beoordelen van het informatiebeveiligings- beleid	IN SCOPE				✓
6 Organiseren van informatiebeveiliging	IN SCOPE				
6.1 Interne organisatie	IN SCOPE				
6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging	IN SCOPE				✓
6.1.2 Scheiding van taken	IN SCOPE				✓
6.1.3 Contact met overheidsinstanties	IN SCOPE		✓	✓	
6.1.4 Contact met speciale belangengroepen	BUITEN SCOPE	Geen speciale groepen van toepassing.			
6.1.5 Informatiebeveiliging in projectbeheer	BUITEN SCOPE	Geen projecten op de productie-omgevingen.			
6.2 Mobiele apparatuur en telewerken	BUITEN SCOPE				
6.2.1 Beleid voor mobiele apparatuur	BUITEN SCOPE	Voor Visibox en Cloudplan is geen mobiele apparatuur in gebruik. Er wordt geen data opgeslagen op mobiele apparatuur. Medewerkers werken via vaste lijnen.			
6.2.2 Telewerken	BUITEN SCOPE	Telewerken gebeurt alleen voor serveronderhoud via een VPN verbinding met het datacenter.			
7 Veilig personeel	IN SCOPE				
7.1 Voorafgaand aan het dienstverband	IN SCOPE				
7.1.1 Screening	IN SCOPE		✓		✓
7.1.2 Arbeidsvoorwaarden	IN SCOPE			✓	
7.2 Tijdens het dienstverband	IN SCOPE				
7.2.1 Directie- verantwoordelijkheden	IN SCOPE				✓
7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	IN SCOPE				✓
7.2.3 Disciplinaire procedures	IN SCOPE				✓
7.3 Beëindiging en wijziging van dienstverband	IN SCOPE				

7.3.1 Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	IN SCOPE				✓
8 Beheer van bedrijfs-middelen	IN SCOPE				
8.1 Verantwoordelijk- heid voor bedrijfsmiddelen	IN SCOPE				
8.1.1 Inventariseren van bedrijfs-middelen	IN SCOPE				✓
8.1.2 Eigendom van bedrijfsmiddelen	IN SCOPE				✓
8.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen	IN SCOPE				✓
8.1.4 Teruggeven van bedrijfsmiddelen	IN SCOPE				✓
8.2 Informatie- classificatie	IN SCOPE				
8.2.1 Classificatie van informatie	IN SCOPE			✓	✓
8.2.2 Informatie labelen	IN SCOPE			✓	✓
8.2.3 Behandelen van bedrijfsmiddelen	IN SCOPE				✓
8.3 Behandelen van media	IN SCOPE				
8.3.1 Beheer van verwijderbare media	IN SCOPE				✓
8.3.2 Verwijderen van media	IN SCOPE				✓
8.3.3 Media fysiek overdragen	IN SCOPE				✓
9 Toegangsbeveiliging	IN SCOPE				
9.1 Bedrijfseisen voor toegangsbeveiliging	IN SCOPE				
9.1.1 Beleid voor toegangsbeveiliging	IN SCOPE		✓		
9.1.2 Toegang tot netwerken en netwerkdiensten	IN SCOPE		✓		
9.2 Beheer van toegangsrechten van gebruikers	IN SCOPE				
9.2.1 Registratie en uitschrijving van gebruikers	IN SCOPE		✓		
9.2.2 Gebruikers toegang verlenen	IN SCOPE		✓		
9.2.3 Beheren van speciale toegangsrechten	IN SCOPE		✓		
9.2.4 Beheer van geheime authenticatie-informatie van gebruikers	IN SCOPE		✓		
9.2.5 Beoordeling van toegangsrechten van gebruikers	IN SCOPE				
9.2.6 Toegangsrechten intrekken of aanpassen	IN SCOPE				✓
9.3 Gebruikers-verantwoordelijkheden	IN SCOPE				
9.3.1 Geheime authenticatie-informatie gebruiken	IN SCOPE				
9.4 Toegangs- beveiliging van systeem en toepassing	IN SCOPE				
9.4.1 Beperking toegang tot informatie	IN SCOPE		✓		
9.4.2 Beveiligde inlogprocedures	IN SCOPE		✓		

9.4.3 Systeem voor wachtwoordbeheer	IN SCOPE		✓		
9.4.4 Speciale systeemhulpmiddelen gebruiken	IN SCOPE				✓
9.4.5 Toegangsbeveiliging op programmabroncode	IN SCOPE		✓		✓
10 Cryptografie	IN SCOPE		✓		
10.1 Cryptografische beheers-maatregelen	IN SCOPE		✓		
10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen	IN SCOPE		✓		
10.1.2 Sleutelbeheer	IN SCOPE		✓		
11 Fysieke beveiliging en beveiliging van de omgeving	IN SCOPE				
11.1 Beveiligde gebieden	IN SCOPE				
11.1.1 Fysieke beveiligingszone	IN SCOPE		✓		
11.1.2 Fysieke toegangsbeveiliging	IN SCOPE		✓		
11.1.3 Kantoren, ruimten en faciliteiten beveiligen	IN SCOPE		✓		
11.1.4 Beschermen tegen bedreigingen van buitenaf	IN SCOPE		✓		
11.1.5 Werken in beveiligde gebieden	IN SCOPE		✓		
11.1.6 Laad- en loslocatie	BUITEN SCOPE	Zowel bij Planning.nl als bij het datacenter geen laad-/loslocatie.			
11.2 Apparatuur	IN SCOPE		✓		
11.2.1 Plaatsing en bescherming van apparatuur	IN SCOPE		✓		
11.2.2 Nutsvoorzieningen	IN SCOPE				
11.2.3 Beveiliging van bekabeling	IN SCOPE		✓		
11.2.4 Onderhoud van apparatuur	IN SCOPE		✓		
11.2.5 Verwijdering van bedrijfsmiddelen	IN SCOPE				
11.2.6 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	IN SCOPE		✓		
11.2.7 Veilig verwijderen of hergebruiken van apparatuur	IN SCOPE		✓		
11.2.8 Onbeheerde gebruikersapparatuur	IN SCOPE		✓		
11.2.9 'Clear desk'- en 'clear screen'-beleid	IN SCOPE		✓		
12 Beveiliging bedrijfs-voering	IN SCOPE				
12.1 Bedieningsprocedures en verantwoordelijkheden	IN SCOPE				
12.1.1 Gedocumenteerde bedieningsprocedures	IN SCOPE				✓
12.1.2 Wijzigingsbeheer	IN SCOPE				✓
12.1.3 Capaciteitsbeheer	IN SCOPE				✓
12.1.4 Scheiding van ontwikkel-, test- en productieomgevingen	IN SCOPE				✓
12.2 Bescherming tegen malware	IN SCOPE				

12.2.1 Beheersmaatregelen tegen malware	IN SCOPE				✓
12.3 Back-up	IN SCOPE				
12.3.1 Backup-up van informatie	IN SCOPE		✓		
12.4 Verslaglegging en monitoren	IN SCOPE				
12.4.1 Gebeurtenissen registreren	IN SCOPE				✓
12.4.2 Beschermen van informatie in logbestanden	IN SCOPE			✓	✓
12.4.3 Logbestanden van beheerders en operators	IN SCOPE				✓
12.4.4 Kloksynchronisatie	IN SCOPE				✓
12.5 Beheersing van operationele software	IN SCOPE				
12.5.1 Software installeren op operationele systemen	IN SCOPE				✓
12.6 Beheer van technische kwetsbaarheden	IN SCOPE				
12.6.1 Beheer van technische kwetsbaarheden	IN SCOPE				✓
12.6.2 Beperkingen voor het installeren van software	IN SCOPE				✓
12.7 Overwegingen betreffende audits van informatie- systemen	IN SCOPE				
12.7.1 Beheersmaatregelen betreffende audits van informatiesystemen	IN SCOPE				✓
13 Communicatie- beveiliging	IN SCOPE				
13.1 Beheer van netwerk- beveiliging	IN SCOPE				
13.1.1 Beheersmaatregelen voor netwerken	IN SCOPE		✓		
13.1.2 Beveiliging van netwerkdiensten	IN SCOPE		✓		
13.1.3 Scheiding in netwerken	IN SCOPE				
13.2 Informatietransport	IN SCOPE				
13.2.1 Beleid en procedures voor informatietransport	IN SCOPE		✓		
13.2.2 Overeenkomsten over informatietransport	IN SCOPE		✓		
13.2.3 Elektronische berichten	IN SCOPE		✓		
13.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst	IN SCOPE		✓		
14 Acquisitie, ontwikke- lingen en onderhoud van informatie- systemen	IN SCOPE				
14.1 Beveiligings- eisen voor informatie- systemen	IN SCOPE				
14.1.1 Analyse en specificatie van informatiebeveiligingseisen	IN SCOPE		✓		

14.1.2 Toepassingsdiensten op openbare netwerken beveiligen	BUITEN SCOPE	Planning.nl levert geen toepassingsdiensten (zoals digitaal financieel transactiebeheer en het leveren van digitale content) op openbare netwerken.			
14.1.3 Transacties van toepassingsdiensten beschermen	BUITEN SCOPE	Planning.nl levert geen toepassingsdiensten (zoals digitaal financieel transactiebeheer en het leveren van digitale content).			
14.2 Beveiliging in ontwikkelings- en ondersteunende processen	IN SCOPE				
14.2.1 Beleid voor beveiligd ontwikkelen	BUITEN SCOPE	Softwareontwikkeling is buiten de scope.			
14.2.2 Procedures voor wijzigingsbeheer met betrekking tot systemen	IN SCOPE		✓		
14.2.3 Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	IN SCOPE				✓
14.2.4 Beperkingen op wijzigingen aan softwarepakketten	IN SCOPE		✓		
14.2.5 Principes voor engineering van beveiligde systemen	IN SCOPE		✓		
14.2.6 Beveiligde ontwikkelomgeving	BUITEN SCOPE	Softwareontwikkeling is buiten de scope.			
14.2.7 Uitbestede softwareontwikkeling	BUITEN SCOPE	Ontwikkelomgeving is buiten scope en softwareontwikkeling is niet uitbesteed.			
14.2.8 Testen van systeembeveiliging	BUITEN SCOPE	Ontwikkelactiviteiten vallen buiten de scope.			
14.2.9 Systeemacceptatietests	IN SCOPE		✓		
14.3 Testgegevens	IN SCOPE				
14.3.1 Bescherming van testgegevens	IN SCOPE			✓	✓
15 Leveranciersrelaties	IN SCOPE				
15.1 Informatie- beveiliging in leveranciers- relaties	IN SCOPE				
15.1.1 Informatiebeveiligingsbeleid voor leveranciersrelaties	IN SCOPE				✓
15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	IN SCOPE				✓
15.1.3 Toeleveringsketen van informatie- en communicatietechnologie	IN SCOPE				✓
15.2 Beheer van dienstverlening van leveranciers	IN SCOPE		✓		
15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers	IN SCOPE		✓		
15.2.2 Beheer van veranderingen in dienstverlening van leveranciers	IN SCOPE		✓		
16 Beheer van informatiebeveiligings-incidenten	IN SCOPE				
16.1 Beheer van informatie-beveiligingsincidenten en -verbeteringen	IN SCOPE				
16.1.1 Verantwoordelijkheden en procedures	IN SCOPE				✓
16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen	IN SCOPE			✓	✓
16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging	IN SCOPE				✓

16.1.4 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	IN SCOPE			✓	✓
16.1.5 Respons op informatiebeveiligingsincidenten	IN SCOPE			✓	✓
16.1.6 Lering uit informatiebeveiligingsincidenten	IN SCOPE				✓
16.1.7 Verzamelen van bewijsmateriaal	IN SCOPE			✓	✓
17 Informatiebeveiligings-aspecten van bedrijfs-continuïteitsbeheer	IN SCOPE		✓		
17.1 Informatie- beveiligings-continuïteit	IN SCOPE		✓		
17.1.1 Informatiebeveiligingscontinuïteit plannen	IN SCOPE		✓		
17.1.2 Informatiebeveiligingscontinuïteit implementeren	IN SCOPE		✓		
17.1.3 Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	IN SCOPE				
17.2 Redundante componenten	IN SCOPE		✓		
17.2.1 Beschikbaarheid van informatieverwerkende faciliteiten	IN SCOPE		✓		
18 Naleving	IN SCOPE				
18.1 Naleving van wettelijke en contractuele eisen	IN SCOPE				
18.1.1 Vaststellen van toepasselijke wetgeving en contractuele eisen	IN SCOPE		✓		
18.1.2 Intellectuele eigendomsrechten	IN SCOPE		✓		
18.1.3 Beschermen van registraties	IN SCOPE		✓		
18.1.4 Privacy en bescherming van persoonsgegevens	IN SCOPE		✓		
18.1.5 Voorschriften voor het gebruik van cryptografische beheersmaatregelen	IN SCOPE		✓		
18.2 Informatiebeveiligings-beoordelingen	IN SCOPE				
18.2.1 Onafhankelijke beoordeling van informatiebeveiliging	IN SCOPE		✓		
18.2.2 Naleving van beveiligingsbeleid en -normen	IN SCOPE		✓		
18.2.3 Beoordeling van technische naleving	IN SCOPE		✓		

Dit document, versie 1.1, is op 12-sep-2017 vastgesteld door de directie van Planning.nl.

Appendix 4: Datacenter en veiligheid

1. Strikte (fysieke) scheiding is tussen de applicatie-, web- en databaseserver

Alle Visibox- en Cloudplan-servers zijn gevirtualiseerd, waarbij web/applicatie en databaseservers gescheiden zijn. De databaseservers zijn ontoegankelijk van buitenaf, communicatie tussen de servers loopt via een zelf-beheerd intern netwerk, is versleuteld en is beperkt tot alleen het noodzakelijke netwerkverkeer.

2. Intrusion Detection Systeem (IDS) en/of een Intrusion Prevention Systeem (IPS)

Verantwoordelijke bepaalt de wachtwoordpolicy voor de eigen gebruikers en kan zelf de complexiteit en geldigheidsduur van wachtwoorden instellen.
Er wordt een Intrusion Detection Systeem (IDS) en een Intrusion Prevention Systeem (IPS) toegepast om ongeautoriseerde loginpogingen te detecteren en te voorkomen.

3. Minimaal 1 keer per jaar onderworpen aan een uitgebreide beveiligingstest

Planning.nl is ISO27001 gecertificeerd en om die reden vindt er eens per 9 maanden een audit plaats. Daarnaast wordt er jaarlijks een penetratietest uitgevoerd door een externe partij. De rapporten hiervan zijn op verzoek ter inzage. De uitkomst wordt gebruikt om de beveiliging van het netwerk te verbeteren. Verder worden alle publiek-toegankelijke servers van Planning.nl dagelijks -geautomatiseerd- gescand op openstaande poorten.

4. Onderhoudswerkzaamheden

Onderhoudswerkzaamheden vinden aangekondigd plaats.
Enkele dagen voor een geplande update wordt een nieuwsbrief verzonden naar alle gebruikers die werken met het pakket waarvoor de update geldt. Hierin wordt verwezen naar een Wiki pagina met een beschrijving van de wijzigingen en/of aanvullingen.

Kleine software updates worden in de regel uitgevoerd volgens parallel deployment, waardoor de gebruiker er praktisch niets van merkt (er hoeven geen servers uitgezet en opnieuw opgestart te worden).
Bij grotere wijzigingen is dat niet altijd mogelijk. In dat geval worden de korte, geplande onderbrekingen die daarvoor nodig zijn via de nieuwsbrief aangekondigd.

5. Twee datacenters redundant uitgevoerd

Planning.nl maakt gebruik van beide datacenters van het eveneens ISO27001 gecertificeerde SmartDC. SmartDC heeft een locatie in Rotterdam en in Heerlen. Bij een calamiteit in Rotterdam kunnen de servers in Heerlen alle Visibox- en Cloudplan-taken overnemen. Als onderdeel van onze ISO27001 certificering zijn hiervoor procedures beschreven die ook worden getest.

6. Datacenter infrastructuur (bron: https://www.smartdc.net/)

6. 1 Informatie over het datacenter

Planning.nl maakt gebruik van de datacenters van SmartDC. De datacenters van SmartDC zijn

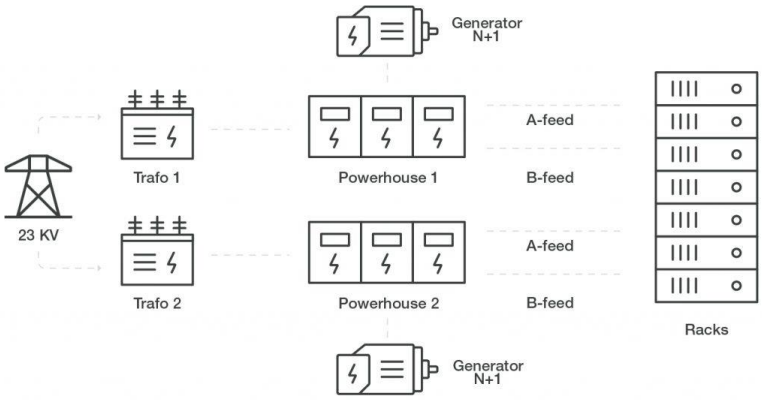
modulair opgebouwd en bestaan uit verschillende suites. Elke suite is een mini-datacenter, met een eigen redundante stroom- en koelvoorziening, zijn eigen glasvezelverbindingen en zijn eigen biometrische toegangscontrole, rookdetectiesysteem en brandblusinstallatie. Toegang tot het datacenter is alleen mogelijk voor geautoriseerde personen en via een vingerscanner. Voor toegang tot het uiteindelijke rack met de servers is naast de vingerafdruk ook een sleutel/toegangscode nodig. SmartDC is ISO27001 en NEN7510 gecertificeerd.

De diensten van Planning.nl worden geleverd vanaf de volgende datacenters:

Primair: Datacenter SmartDC Rotterdam (*https://www.smartdc.net/nl/rotterdam/*)
Secundair: Datacenter SmartDC Heerlen (*https://www.smartdc.net/nl/heerlen/*)

6.2 Stroomvoorziening

De stroomvoorzieningen van beide datacenters zijn redundant uitgevoerd. Elk server-rack heeft meerdere, van elkaar onafhankelijke stroomvoorzieningen. Deze stroomvoorzieningen worden gevoed vanuit het elektriciteitsnet met als back-up een UPS en eigen dieselgeneratoren die ervoor zorgen dat het datacenter nooit zonder stroom komt te zitten.



Figuur 1. Schematische weergave stroomvoorziening co-locatie Rotterdam

Het datacenter in Rotterdam voldoet aan alle voorwaarden voor een TIER-IV certificering waarvoor een uptime van 99.995% is vereist. Dit is de hoogst haalbare norm voor datacenters in het classificatiesysteem van het Uptime Institute. SmartDC Rotterdam heeft sinds de oprichting een uptime van 99.9999%, en het datacenter in Heerlen heeft zelfs 100% uptime.

6.3 Netwerken, verbindingen en redundantie

De publiek toegankelijke servers zijn via een gigabit netwerk met het internet verbonden. De hostinglocaties zijn onderling verbonden via een gigabit MPLS, waardoor de servers in Heerlen de taken kunnen overnemen van die in Rotterdam (en andersom). De Visibox- en Cloudplan-servers zijn gevirtualiseerd, geclusterd en geconfigureerd in load-balancing en fail-over mode. Dit komt de performance en betrouwbaarheid ten goede. Door de fail-over mode kunnen servers bij uitval elkaars taken automatisch overnemen zonder dat de eindgebruiker hier iets van merkt.
Naast de virtuele servers zijn ook de fysieke servers (waar de virtuele servers op draaien) redundant uitgevoerd en geconfigureerd in een fail-over cluster. Ook hier zal bij uitval van een fysieke server (of als deze onbereikbaar is) een andere server automatisch de taken overnemen. Alle servers worden continu gemonitord om problemen voor te zijn of snel op te kunnen lossen.
Beide datacenters (Rotterdam & Heerlen) kunnen elkaars taken overnemen en doen dit (gedeeltelijk) automatisch.

7. Back-up

Alle databases worden iedere nacht geback-upt. Dit zijn volledige back-ups (en geen ‘incremental back-ups’). Een geautomatiseerd systeem controleert iedere morgen of de back-ups gemaakt zijn, de juiste grootte hebben en op de juiste plekken staan. Deze back-ups zijn voorzien van een sterke encryptie en onbruikbaar zonder de encryptiesleutels. De back-ups worden 14 dagen bewaard en op meerdere locaties. Op verzoek kunnen back-ups langer worden bewaard.
Op verzoek kunnen gegevens uit een back-up teruggelezen worden. Hiervoor is een schriftelijk verzoek nodig (bv per mail) bij een supportmedewerker, die bij twijfel (bv over of de persoon gemachtigd is om het verzoek te doen) contact op zal nemen met de contactpersoon van de klant.

8. Beveiliging op het hoogste niveau

Planning.nl neemt het onderwerp informatiebeveiliging zeer serieus en conformeert zich aan de ISO 27001:2013 norm (en is dan ook ISO 27001:2013 gecertificeerd). Ook het SmartDC datacenter is ISO 27001 gecertificeerd (en NEN7510 gecertificeerd)

9. Beveiligingsmissie van Planning.nl

Planning.nl hanteert de volgende beleidsprincipes m.b.t. informatiebeveiliging:

- Planning.nl beschermt aantoonbaar de gegevens van de klant, zodat de klant op verantwoorde wijze gebruik kan maken van de door Planning.nl aangeboden SAAS-oplossing.
- Planning.nl vindt het belangrijk dat het beveiligingsbeleid gedragen wordt door alle medewerkers binnen het bedrijf.
- Bij de ontwikkeling, aanschaf en uitfasering van informatiesystemen dient nadrukkelijk aandacht besteed te worden aan informatiebeveiliging.
- Planning.nl voldoet aan de AVG.