



Suits Group

Data Processing Terms (verwerkersvoorwaarden)

Suits Data Processing Terms (verwerkersvoorwaarden)

Suits group · Versie 1.0 · in werking vanaf 1 november 2026

Deze Data Processing Terms gelden wanneer een Suits Entity persoonsgegevens namens jou verwerkt als verwerker. Ze maken deel uit van de Overeenkomst, zoals bepaald in artikel 14.2 van de Group Master Terms. Termen met een hoofdletter hebben de betekenis die de Group Master Terms of de Algemene Verordening Gegevensbescherming ("AVG") eraan geven.

1. Wanneer deze voorwaarden gelden

1.1 Voor de meeste van onze Diensten bepalen wij zelf hoe en waarom wij persoonsgegevens verwerken, bijvoorbeeld om aan onze professionele en wettelijke verplichtingen te voldoen. Voor die verwerking zijn wij verwerkingsverantwoordelijke en geldt ons privacybeleid.

1.2 Deze voorwaarden gelden alleen wanneer wij persoonsgegevens namens jou en volgens jouw instructies verwerken. Bijlage A vermeldt de Diensten waarvoor dat het geval is.

1.3 Wanneer het recht van het Verenigd Koninkrijk op de verwerking van toepassing is, omvatten verwijzingen naar de AVG ook de UK GDPR en de Data Protection Act 2018. Wanneer het recht van de Verenigde Arabische Emiraten van toepassing is, omvatten zij ook de UAE Personal Data Protection Law, voor zover die van toepassing is.

2. Jouw instructies

2.1 Wij verwerken de persoonsgegevens uitsluitend op basis van jouw schriftelijke instructies. De Overeenkomst, de Commerciële Afspraak en deze voorwaarden zijn jouw instructies. Verdere instructies moeten schriftelijk worden gegeven.

2.2 Wij laten je weten als een instructie naar ons oordeel inbreuk maakt op de gegevensbeschermingswetgeving. Wij mogen die instructie dan opschorten.

2.3 Wij mogen de persoonsgegevens zonder jouw instructie verwerken wanneer de wet dat vereist, zoals de antiwitwaswetgeving. Wanneer de wet het toelaat, laten wij je dat weten voordat wij dat doen.

2.4 Jij bent verantwoordelijk voor een rechtmatige grondslag voor de verwerking en voor het informeren van de betrokkenen.

3. Vertrouwelijkheid en beveiliging

3.1 Iedereen die de persoonsgegevens voor ons verwerkt, is tot geheimhouding verplicht.

3.2 Wij nemen de technische en organisatorische maatregelen die in Bijlage B zijn beschreven om de persoonsgegevens te beschermen. Wij mogen deze maatregelen wijzigen, op voorwaarde dat het beschermingsniveau niet daalt.

4. Subverwerkers

4.1 Je geeft ons een algemene toestemming om subverwerkers in te schakelen. Dit omvat groepsvennootschappen, onze backoffice en aanbieders van standaard bedrijfssoftware en zakelijke diensten, zoals e-mail- en kantoorsoftware, boekhoud- en loonsoftware, cliëntbeheer, elektronische handtekening, communicatietools, tools voor artificiële intelligentie onder zakelijke voorwaarden, cloudopslag en hosting. De actuele lijst staat op suitsfinance.com/terms.

4.2 Wij informeren je over een nieuwe of vervangende subverwerker door die lijst ten minste veertien dagen vóór de wijziging bij te werken. Op verzoek informeren wij je ook per e-mail. Je kunt binnen die termijn schriftelijk bezwaar maken, op redelijke gronden van gegevensbescherming. Een bezwaar houdt de wijziging niet tegen. Als wij niet aan je bezwaar tegemoet kunnen komen, mag je de betrokken Dienst beëindigen, zonder vergoeding.

4.3 Wij leggen elke subverwerker dezelfde verplichtingen inzake gegevensbescherming op als in deze voorwaarden. Wij blijven tegenover jou verantwoordelijk voor de nakoming door onze subverwerkers.

5. Doorgiften buiten de Europese Economische Ruimte

5.1 Wij geven de persoonsgegevens alleen door buiten de Europese Economische Ruimte of het Verenigd Koninkrijk wanneer de AVG dat toelaat, zoals beschreven in afdeling 8 van ons privacybeleid. Waar nodig sluiten wij modelcontractbepalingen (SCC's) met de ontvanger, ook met onze groepsvennootschappen en onze backoffice.

6. Bijstand

6.1 Wij helpen je, rekening houdend met de aard van de verwerking en de informatie waarover wij beschikken:

6.1.1 bij het beantwoorden van verzoeken van betrokkenen. Als wij zo'n verzoek rechtstreeks ontvangen, sturen wij het zonder onredelijke vertraging aan jou door;

6.1.2 bij gegevensbeschermingseffectbeoordelingen en voorafgaande raadplegingen van een toezichthoudende autoriteit;

6.1.3 bij het nakomen van je verplichtingen inzake beveiliging en inbreuken in verband met persoonsgegevens (datalekken).

6.2 Bijstand die verder gaat dan wat redelijk is voor de Dienst, is meerwerk tegen ons uurtarief.

7. Inbreuken in verband met persoonsgegevens

7.1 Wij informeren je zonder onredelijke vertraging nadat wij kennis hebben gekregen van een inbreuk in verband met persoonsgegevens die de persoonsgegevens treft, en in elk geval binnen 48 uur.

7.2 Wij geven je de informatie waarover wij beschikken en die je nodig hebt om de toezichthoudende autoriteit en de betrokkenen in kennis te stellen. Als wij niet meteen over alle informatie beschikken, verstrekken wij die in fasen.

8. Audits

8.1 Wij stellen je de informatie ter beschikking die nodig is om aan te tonen dat deze voorwaarden worden nageleefd.

8.2 Je mag een audit uitvoeren, zelf of via een auditor die je daartoe aanstelt, beiden gebonden door geheimhouding, ten hoogste eenmaal per jaar, na een schriftelijke aankondiging van ten minste dertig dagen, en daarnaast na een inbreuk in verband met persoonsgegevens die jouw persoonsgegevens treft of op verzoek van een toezichthoudende autoriteit. De audit vindt plaats tijdens de kantooruren, verstoort ons werk niet en tast de vertrouwelijkheid van andere cliënten niet aan. Je draagt de kosten ervan, tenzij de audit een wezenlijke schending van deze voorwaarden door ons aantoont.

9. Einde van de verwerking

9.1 Wanneer de Dienst eindigt, verwijderen wij de persoonsgegevens of geven wij ze terug, naar jouw keuze. Artikel 10.7 van de Group Master Terms is niet van toepassing op persoonsgegevens die wij namens jou verwerken. Als je niet binnen dertig dagen na het einde kiest, verwijderen wij ze.

9.2 Wij mogen persoonsgegevens bewaren wanneer de wet ons daartoe verplicht, zoals fiscale wetgeving en antiwitwaswetgeving, of wanneer wij ze nodig hebben om een rechtsvordering in te stellen, uit te oefenen of te verdedigen, zolang zo'n vordering mogelijk is. Voor die gegevens zijn wij verwerkingsverantwoordelijke en geldt ons privacybeleid.

10. Aansprakelijkheid

10.1 Artikel 17 van de Group Master Terms is van toepassing op alle vorderingen op grond van deze voorwaarden, voor zover de wet dat toelaat.

11. Rangorde

11.1 Als deze voorwaarden in strijd zijn met de Group Master Terms, de Annex of de Opdrachtbrief (engagement letter) wat betreft de verwerking van persoonsgegevens als verwerker, gaan deze voorwaarden voor. Op alle andere punten is artikel 3 van de Group Master Terms van toepassing.

Bijlage A: Diensten waarvoor wij verwerker zijn

Dienst	Suits Entity	Betrokkenen	Persoonsgegevens
Loonadministratie	Suits Finance B.V., Suits Finance Accountants BV, SUITS FINANCE - FZCO	Je werknemers, bestuurders en voormalige werknemers	Identiteits- en contactgegevens, nationaal identificatienummer, arbeids- en loongegevens, bankrekeningnummer, verzuimgegevens die nodig zijn voor de loonverwerking
Boekhouding	Suits Finance B.V., Suits Finance Accountants BV, SUITS FINANCE UK LTD, SUITS FINANCE - FZCO	Je klanten, leveranciers en werknemers, zoals zij in je boekhouding voorkomen	Namen, contactgegevens, factuur- en betalingsgegevens, bankrekeningnummers

Doel: het uitvoeren van de betrokken Dienst. Duur: de looptijd van de Dienst, gevolgd door artikel 9.

Bijlage B: Technische en organisatorische maatregelen

1. Toegangsbeheer

1.1 Toegang tot ons cliëntbeheersysteem (Odoo) wordt verleend per rol en per Suits Entity. Een gebruiker heeft alleen toegang tot de Suits Entities die voor die gebruiker zijn ingesteld.

1.2 Toegang tot Microsoft 365 en SharePoint verloopt via persoonlijke accounts en via groepen per Suits Entity. Mappen van finance en management zijn alleen toegankelijk voor een beperkte groep.

1.3 Toegang tot onze boekhoud- en belastingsoftware wordt verleend per rol en per Suits Entity, met vaste rechten per rol. In Yuki wordt toegang verleend per administratie. De beheerder van elk pakket maakt op verzoek van de leidinggevende een persoonlijk account aan.

1.4 Een leidinggevende vraagt elk nieuw account aan en IT maakt het aan. Wanneer iemand vertrekt, wordt het account op de laatste werkdag geblokkeerd, worden sessies en authenticatiemethoden ingetrokken, en controleert IT dit de volgende werkdag.

1.5 Personeelsdossiers met identiteitsdocumenten van onze eigen Medewerkers zijn alleen toegankelijk voor HR en management.

1.6 Toegang tot ons archief van chats met cliënten is beperkt tot een vaste groep Medewerkers die zich aanmelden met hun Microsoft-account van Suits. Elke toegang wordt gelogd.

2. Authenticatie

2.1 Meerfactorauthenticatie is verplicht voor Microsoft 365, Xero en Zoho. Voor Microsoft 365 wordt dit afgedwongen via voorwaardelijke toegang (conditional access), en aanmelden met verouderde protocollen is geblokkeerd.

2.2 Apparaten die in Microsoft Intune worden beheerd, vereisen een sterk wachtwoord of een sterke toegangscode.

3. Apparaten

3.1 Laptops en telefoons die in Microsoft Intune worden beheerd, kunnen bij verlies of diefstal op afstand worden gewist.

3.2 Mac-computers en iPhones die in Microsoft Intune worden beheerd, zijn versleuteld.

4. Uitwisseling van documenten

4.1 Documenten ter ondertekening worden uitgewisseld via Odoo Sign. Wij vragen informatie op via beveiligde formulieren en ons cliëntportaal.

5. Back-ups

5.1 Van onze eigen servers wordt dagelijks een back-up gemaakt. Back-ups worden zeven dagen bewaard, lokaal en op een externe locatie in de Europese Unie.

5.2 De aanbieders van ons cliëntbeheersysteem, Yuki en Xero maken back-ups van de gegevens die zij voor ons hosten.

6. Logging

6.1 Aanmeldingen, mailboxactiviteit en beheerwijzigingen in Microsoft 365 worden gelogd. De centrale auditlog wordt 180 dagen bewaard.

6.2 Ons cliëntbeheersysteem registreert elke gebruikerssessie met het apparaat, het IP-adres en het land, en bewaart per record een wijzigingsgeschiedenis zolang het record bestaat.

7. Bewustwording

7.1 Onze Medewerkers hebben toegang tot interne richtlijnen over IT en gegevensbescherming en tot een formulier om phishing te melden. Nieuwe Medewerkers krijgen op hun eerste werkdag een introductie.

8. Fysieke beveiliging

8.1 Wij bewaren alle cliëntdossiers digitaal. Wij bewaren geen papieren cliëntdossiers.