



Suits Group

Data Processing Terms

Suits Data Processing Terms

Suits group · Version 1.0 · effective from 1 November 2026

These Data Processing Terms apply where a Suits Entity processes personal data on your behalf as a processor. They form part of the Agreement, as set out in Article 14.2 of the Group Master Terms. Capitalised terms have the meaning given to them in the Group Master Terms or in the General Data Protection Regulation ("GDPR").

1. When these terms apply

1.1 For most of our Services, we decide ourselves how and why we process personal data, for example to meet our professional and legal obligations. For that processing we are a controller and our Privacy Policy applies.

1.2 These terms apply only where we process personal data on your behalf and under your instructions. Schedule A lists the Services for which that is the case.

1.3 Where the law of the United Kingdom applies to the processing, references to the GDPR include the UK GDPR and the Data Protection Act 2018. Where the law of the United Arab Emirates applies, they include the UAE Personal Data Protection Law, to the extent it applies.

2. Your instructions

2.1 We process the personal data only on your documented instructions. The Agreement, the Commercial Agreement and these terms are your instructions. Further instructions must be given in Writing.

2.2 We tell you if, in our opinion, an instruction infringes data protection law. We may then suspend that instruction.

2.3 We may process the personal data without your instruction where the law requires it, such as anti money laundering law. Where the law allows it, we tell you before we do so.

2.4 You are responsible for having a lawful basis for the processing and for informing the data subjects.

3. Confidentiality and security

3.1 Everyone who processes the personal data for us is bound by confidentiality.

3.2 We take the technical and organisational measures described in Schedule B to protect the personal data. We may change these measures, provided the level of protection does not decrease.

4. Sub-processors

4.1 You give us general authorisation to engage sub-processors. This includes Group Companies, our back office, and providers of standard business software and services, such as email and office software, accounting and payroll software, client management, electronic signature, communication tools, artificial intelligence tools under business terms, cloud storage and hosting. The current list is available at suitsfinance.com/terms.

4.2 We inform you of a new or replacement sub-processor by updating that list at least fourteen days before the change. On request, we also inform you by email. You may object in Writing within that period, on reasonable data protection grounds. An objection does not prevent the change. If we cannot meet your objection, you may terminate the Service concerned, without compensation.

4.3 We impose on each sub-processor the same data protection obligations as in these terms. We remain responsible to you for the performance of our sub-processors.

5. Transfers outside the European Economic Area

5.1 We only transfer the personal data outside the European Economic Area or the United Kingdom where the GDPR allows it, as described in section 8 of our Privacy Policy. Where needed, we conclude standard contractual clauses with the recipient, including with our Group Companies and our back office.

6. Assistance

6.1 We assist you, taking into account the nature of the processing and the information available to us:

6.1.1 in responding to requests from data subjects. If we receive such a request directly, we forward it to you without undue delay;

6.1.2 with data protection impact assessments and prior consultations with a supervisory authority;

6.1.3 in meeting your obligations on security and personal data breaches.

6.2 Assistance beyond what is reasonable for the Service is additional work at our hourly rate.

7. Personal data breaches

7.1 We inform you without undue delay after we become aware of a personal data breach affecting the personal data, and in any event within 48 hours.

7.2 We give you the information we have and that you need to notify the supervisory authority and the data subjects. If we do not have all information at once, we provide it in phases.

8. Audits

8.1 We make available to you the information needed to demonstrate compliance with these terms.

8.2 You may carry out an audit, yourself or through an auditor you mandate, both bound by confidentiality, at most once a year, after at least thirty days' notice in Writing, and additionally after a personal data breach affecting your personal data or at the request of a supervisory authority. The audit takes place during office hours and does not disrupt our work or affect the confidentiality of other clients. You bear its costs, unless the audit shows a material breach of these terms by us.

9. End of the processing

9.1 When the Service ends, we delete or return the personal data, at your choice. Article 10.7 of the Group Master Terms does not apply to personal data we process on your behalf. If you do not choose within thirty days after the end, we delete it.

9.2 We may keep personal data where the law requires us to, such as tax and anti money laundering law, or where we need it to establish, exercise or defend a legal claim, for as long as such a claim is possible. For that data we are a controller and our Privacy Policy applies.

10. Liability

10.1 Article 17 of the Group Master Terms applies to all claims under these terms, to the extent the law allows.

11. Order of precedence

11.1 If these terms conflict with the Group Master Terms, the Annex or the Engagement Letter on the processing of personal data as a processor, these terms prevail. On all other points, Article 3 of the Group Master Terms applies.

Schedule A: Services for which we are a processor

Service	Suits Entity	Data subjects	Personal data
Payroll administration	Suits Finance B.V., Suits Finance Accountants BV, SUITS FINANCE - FZCO	Your employees, directors and former employees	Identity and contact data, national identification number, employment and salary data, bank account number, absence data needed for payroll
Bookkeeping	Suits Finance B.V., Suits Finance Accountants BV, SUITS FINANCE UK LTD, SUITS FINANCE - FZCO	Your customers, suppliers and employees, as they appear in your bookkeeping records	Names, contact data, invoice and payment data, bank account numbers

Purpose: performing the Service concerned. Duration: the term of the Service, followed by section 9.

Schedule B: Technical and organisational measures

1. Access control

1.1 Access to our client management system (Odoo) is granted per role and per Suits Entity. A user only has access to the Suits Entities set for that user.

1.2 Access to Microsoft 365 and SharePoint runs through personal accounts and through groups per Suits Entity. Folders of finance and management are only accessible to a limited group.

1.3 Access to our accounting and tax software is granted per role and per Suits Entity, with fixed rights per role. In Yuki, access is granted per administration. The administrator of each package creates a personal account at the request of the manager.

1.4 A manager requests every new account, and IT creates it. When someone leaves, the account is blocked on the last working day, sessions and authentication methods are revoked, and IT checks this the next working day.

1.5 Personnel files with identity documents of our own staff are only accessible to HR and management.

1.6 Access to our archive of client chats is limited to a fixed group of staff who sign in with their Suits Microsoft account. Every access is logged.

2. Authentication

2.1 Multi factor authentication is mandatory for Microsoft 365, Xero and Zoho. For Microsoft 365 it is enforced through conditional access, and sign in with legacy protocols is blocked.

2.2 Devices managed in Microsoft Intune require a strong password or passcode.

3. Devices

3.1 Laptops and phones managed in Microsoft Intune can be wiped remotely in case of loss or theft.

3.2 Mac computers and iPhones managed in Microsoft Intune are encrypted.

4. Exchange of documents

4.1 Documents for signature are exchanged through Odoo Sign. We request information through secured forms and our client portal.

5. Back ups

5.1 Our own servers are backed up daily. Back ups are kept for seven days, locally and at an external location in the European Union.

5.2 The providers of our client management system, Yuki and Xero make back ups of the data they host for us.

6. Logging

6.1 Sign ins, mailbox activity and administrative changes in Microsoft 365 are logged. The central audit log is kept for 180 days.

6.2 Our client management system records each user session with the device, IP address and country, and keeps a change history per record for as long as the record exists.

7. Awareness

7.1 Our staff have access to internal guidance on IT and data protection and to a form to report phishing. New staff receive an introduction on their first working day.

8. Physical security

8.1 We keep all client files digitally. We do not keep paper client files.