Updated April 30, 2026

Data Processing Addendum

Operative Provisions

1. **Definitions**. Under these Terms, **Personal Data** is information defined as personal data, personal information, or an equivalent term under relevant Data Protection Laws, processed by You or Remote Europe in connection with these Terms. **Data Protection Laws** means all applicable data protection and privacy laws, rules, regulations, governmental orders, and subordinate legislation, now or hereafter in force, applicable to a party in the performance of its obligations or exercise of its rights under these Terms, such as Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (**EU GDPR**), or the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (**UK GDPR**). **Personal Data Breach** is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. **Adequate Country** means a country or territory that a relevant authority such as the European Commission or a national data protection authority has recognised under applicable Data Protection Laws as providing adequate level of protection for the international transfer of Personal Data.
2. **Roles of the parties**. The parties acknowledge that with respect to the processing by each party of any Personal Data with regard to Employment Services, each party shall act as an independent Controller. The details of the processing are set out in Schedule 1 of this DPA.
   The parties acknowledge that with respect to the processing by each party of any Personal Data with regard to Contractor of Record Services, each party shall act as an independent Controller. The details of the processing are set out in Schedule 5 of this DPA.
   You agree that You are responsible for compliance with Data Protection Laws with respect to all Personal Data Your authorised users upload on and download from our Platform and how they use such Personal Data. Where You use Payroll Services, HRIS, Contractor Management Services, Mobility as a Service and/or Perform, We process the relevant Personal Data on Your behalf, in line with section 7 of this DPA, and We act as Processor. The details of processing for our role as a Processor are set out in Schedules 2, 3, 4, 6 and 7 respectively to this DPA.
   Where You use Our Remote Recruit Service, We process personal data of candidates registered on remote.com/jobs and We act as a Controller for their data. You are responsible for the personal data of registered candidates who apply to Your job posting on Remote Recruit and for candidates' personal data You get access to in Remote Recruit. You agree that You are responsible for the compliance under the applicable Data Protection Laws regarding the collected personal data of all such candidates.
   Where You use Perform, We process the relevant Personal Data on Your behalf and We

act as Processor in line with section 7 of this DPA. The details of processing for our role as a Processor are set out in Schedule 6 of this DPA.

3. **Term and data retention**. After termination of the Terms, Personal Data shall be retained by the parties for no longer than the maximum retention period applicable to such Personal Data, as set out in applicable national laws. This DPA shall remain in force for as long as the parties retain Personal Data. For the avoidance of doubt, We will retain Personal Data that is relevant to the Terms of Service provisions that survive termination for as long as those provisions survive. In addition, We will retain Personal Data that is necessary to enforce Our legal rights such as those rights contained in any non-disclosure agreements between Us and the Employees, Consultants and Contractors.

1. **Mutual cooperation**. Each party will implement appropriate technical and organisational measures to ensure the security of the Personal Data. Each party will provide reasonable cooperation and assistance to the other party as may be necessary to enable such other party to: (i) comply with any obligations of such other party under Data Protection Laws, (ii) facilitate the handling by the other party of any actual or reasonably suspected Personal Data Breach, (iii) comply in any investigations or audits by a regulator or supervisory authority. To the extent either party makes available to the other party any Personal Data in connection with this Agreement prior to making available any Personal Data, the disclosing party shall comply with any applicable consent, transparency and disclosure requirements under Data Protection Laws with respect to such Personal Data.
2. **Processors**. Each party warrants and undertakes that it shall comply (and contractually require their agents, service providers, Processors or subcontractors to comply) with applicable Data Protection Laws. Each party is and shall remain independently responsible for the processing it carries out as Controller whether on its own or through its Processors.
3. **International transfers**. If We are certified to the EU-U.S. Data Privacy Framework, Swiss-US Data Privacy Framework and/or UK Extension to the EU-US Data Privacy Framework (as applicable), the parties agree that for so long as We are so certified, the relevant framework as applicable will apply to relevant transfers of data to Us. Where the EU GDPR applies, and Personal Data is transferred to a country other than an Adequate Country or to an entity other than certified under the EU-U.S. Data Privacy Framework, Swiss-US Data Privacy Framework and/or UK Extension to the EU-US Data Privacy Framework (as applicable), the Standard Contractual Clauses in the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN) (**EU SCCs**) shall apply to such transfers. Where the UK GDPR applies, and Personal Data is transferred to a country other than an Adequate Country or to an entity other than certified under the EU-U.S. Data Privacy Framework, Swiss-US Data Privacy Framework and/or UK Extension to the EU-US Data Privacy Framework (as applicable), then the EU SCCS shall apply and the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 (**UK Addendum**) shall apply to

all such transfers; and each shall be fully incorporated into this DPA and deemed completed as set out below:

a. When We disclose Personal Data subject to the Data Protection Laws to You and You receive such Personal Data outside an Adequate Country, We shall act as the Data exporter.
b. When You disclose Personal Data subject to Data Protection Laws to Us and We receive such Personal Data outside an Adequate Country, We shall act as the Data importer.
c. Where We act as independent Controllers in relation to Personal Data protected by the EU GDPR, Module 1 of the EU SCCs will apply as follows:

(i) Clause 7 (Docking Clause) shall not apply,

(ii) the optional language in Clause 11 (Redress) shall not apply.

(iii) For Clause 13 (Supervision), the supervisory authority with responsibility for ensuring compliance by the data exporter with the GDPR with regard to restricted transfers shall be the Dutch supervisory authority;

(iv) For Clause 17 (Governing Law), Option 1 shall apply and the EU SCCs shall be governed by the laws of the Netherlands.

(v) For Clause 18 (Choice of forum and jurisdiction), the Parties agree that the courts of the Netherlands shall resolve any disputes arising out of the EU SCCs.

(vi) The information required by Annex I of the EU SCCs is set out in Schedule 8 of this DPA.

(vii) The information required by Annex II of the EU SCCs is set out in Schedule 8 of this DPA.

d. Where We act as independent Controllers in relation to Personal Data protected by the UK GDPR, the parties agree that the UK Addendum will apply completed as follows: the EU SCCs shall apply completed as set out in section 6(a) and shall also apply to transfers of such Personal Data. In addition, tables 1 to 3 of the UK Addendum shall be deemed completed with the relevant information from the EU SCCs, completed as set out above in section 6(a) and table 4 shall be deemed completed by selecting "neither party". The start date of the UK Addendum (as set out in Table 1) shall be the date of this DPA.

e. Where We act as a Processor for You as Controller in relation to Personal Data protected by the EU GDPR, Module 2 of the EU SCCs will apply as follows:

(i) Clause 7 (Docking Clause) shall not apply,

(ii) the Clause 9 (Use of sub-Processors) Option 2 - General written authorisation shall apply with 14 days' time to object to the changes.

(iii) the optional language in Clause 11 (Redress) shall not apply.

(iv) For Clause 13 (Supervision), the supervisory authority with responsibility for ensuring compliance by the data exporter with the GDPR with regard to restricted transfers shall be the Dutch supervisory authority;

(v) For Clause 17 (Governing Law), Option 1 shall apply and the EU SCCs shall be governed by the laws of the Netherlands.

(vi) For Clause 18 (Choice of forum and jurisdiction), the Parties agree that the courts of the Netherlands shall resolve any disputes arising out of the EU SCCs.

(vii) The information required by Annex I of the EU SCCs is set out in Schedule 8 of this DPA.

(viii) The information required by Annex II of the EU SCCs is set out in Schedule 8 of this DPA.

f. Where We act as a Processor for You as Controller in relation to Personal Data protected by the UK GDPR, the parties agree that the UK Addendum will apply completed as follows: the EU SCCs shall apply completed as set out in section 6(c) and shall also apply to transfers of such Personal Data. In addition, tables 1 to 3 of the UK Addendum shall be deemed completed with the relevant information from the EU SCCs, completed as set out above in section 6(c) and table 4 shall be deemed completed by selecting "neither party". The start date of the UK Addendum (as set out in Table 1) shall be the date of this DPA.

7. **Remote as a Processor**. Where Remote acts as a Processor and You act as a Controller in connection with the Services, the following additional terms shall apply:

7.1 **Compliance and instructions**. You and Us will comply with all requirements of all relevant Data Protection Laws, as applicable to the provision and receipt of the Services and as applicable to our roles for data protection purposes. Where you act as Controller and We act as Processor We will process Personal Data only to the extent necessary to perform Our obligations pursuant to these Terms and in accordance with Your documented instructions. As soon as reasonably practicable upon becoming aware, We shall inform You if, in Our opinion, any instructions provided by You under this DPA infringe Data Protection Laws, but without obligation to actively monitor Your compliance with Data Protection Laws.

Where You instruct Us to process any additional Personal Data not covered by this DPA on Your behalf directly via the Platform, We will act as Processor regarding such processing under the GDPR. The details of the processing will depend on the nature and purpose of Your Platform request. In such cases clauses 7.3 - 7.9 of this DPA will apply accordingly.

7.2 **Details of processing**. The subject matter of the processing, its purpose, duration and means, together with the relevant categories of Personal Data and data subjects are set out at Schedules 2 to 4, 6 and 7 incl. to this DPA.

7.3 **Sub-Processors**. You hereby provide Us with a general authorisation to engage sub-Processors as necessary to deliver the Services provided that: (i) We commit to informing You of any intended changes concerning the addition or replacement of Processors, by way of updating Our Processor list, available here: https://employ.remote.com/dashboard/processors (for registered users only) thereby giving You an opportunity to object to such changes, within 14 days following notification of such an update or change to the Processor list. We shall produce an up-to-date list of sub-Processors engaged by Us to deliver the Services to You without undue delay upon written request; (ii) We impose data protection terms on any sub-Processors We appoint that protect the Personal Data, in substance, to the same standard provided for by this section 7.

7.4 **Our personnel**. We warrant that the personnel We engage to process Personal Data on Your behalf in connection with the Services are informed of their obligations in relation to Personal Data, and that they will process Personal Data in confidentiality and in accordance with these Terms and all relevant data protection legislation.

7.5 **Security of processing**. We shall implement technical and organisational measures to keep Personal Data processed in connection with the Services secure against unauthorised or unlawful processing and against accidental loss, destruction or damage. The applicable technical and organisational measures related to security are specified at Schedule 9 to this DPA.

We will notify You without undue delay but no later than in 72 hours after ascertaining that there has been a Personal Data Breach and provide reasonable information in Our possession to assist You to meet Your obligations to report a Personal Data Breach as required under applicable Data Protection Laws.

7.6 **Processor assistance**. We shall assist You in responding to any requests made by relevant data subjects which concern the exercise of their rights under Data Protection Laws. We shall promptly notify You if We receive a data subject request in connection with Services where we act as Processor. In such circumstances We shall not respond to a data subject request received by Remote without Your consent (not to be unreasonably withheld). We will also assist You, to the extent necessary, in relation to data protection impact assessments and prior consultations with data protection authorities. We will make available to You all information necessary to demonstrate compliance with the obligations laid out in this section 7.

7.7 **Audit rights**. Unless We carry out an audit for Our compliance with Data Protection Laws, either independently or via a third party and share the results of such audit with You, then You or Your independent third-party auditor may audit Our compliance with obligations under applicable Data Protection Laws, at most once in 12 consecutive months, where: a) You provide reasonable grounds to believe that Remote is in breach of its

obligation(s) under the applicable Data Protection Laws and this section 7; b) You provide reasonable grounds to believe that a Personal Data breach has occurred; or c) an audit is formally requested by a data protection authority. You shall provide at least thirty days' advance notice of any audit unless mandatory applicable Data Protection Laws or a competent data protection authority requires shorter notice or unless a Personal Data breach is alleged, where a shorter notice period can be provided. The scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Each party shall bear its costs of audits hereunder.

7.8 **International onward transfers**. We will transfer Personal Data internationally, to all our Affiliates and to all sub-Processors, at all times subject to compliance with Data Protection Laws. If We transfer Personal Data that is protected by the EU GDPR and/or UK GDPR, We shall do so only in compliance with such laws, and if Personal Data is transferred to a country other than an Adequate Country or an entity other than certified under the EU-U.S. Data Privacy Framework, Swiss-US Data Privacy Framework and/or UK Extension to the EU-US Data Privacy Framework (as applicable), pursuant to the EU SCCs and/or UK Addendum (as applicable) implemented between the relevant exporter and importer of the Personal Data.

7.9 **Termination obligations**. Upon termination of the commercial relationship between Us and You, We will, at Your choice, delete or return all the Personal Data processed on Your behalf in connection with the Services to You and delete existing copies unless otherwise required by applicable law, in which case We shall isolate and protect the Personal Data from any further processing to the extent required by such law until deletion is possible.

Schedule 1 - Standard and Premium Employment Services

1. Roles

Each party acts as an independent Controller in the context of Standard and Premium Employment Services and shall process Personal Data in compliance with applicable Data Protection Laws and these Terms.2. Categories of data subjects whose Personal Data is processed

- Employees, Consultants assigned to You, and
- Authorised users of the Remote Platform engaged by You.

3. Categories of Personal Data processed

- In relation to Employees and Consultants: personal identification data, address data, contact data, administrative data, emergency person contact data, contract data, time off data, feedback data, employment data, custom fields data, data in documents, payment and tax data.

- In relation to Your authorised users: authorised-user-generated access credentials, email address and the content of communications relating to their use of the Remote platform.
- Any other categories of Personal Data agreed to be processed by the parties in writing and/or required by law.

4. Sensitive data processed

- Data concerning health, processing of which is necessary for the purpose of carrying out obligations and exercising specific rights of the Controller or data subject in the field of employment;
- Biometric data for the purpose of identity verification of a natural person.

5. The frequency of the transfer

- Personal Data is transferred on a continuous basis.

6. Nature of the processing

- Personal Data will be processed as follows:
    - authorised users will be appointed by You and invited to the Platform,
    - You will onboard Employees/Consultants on the Platform,
    - Employees/Consultants will submit their onboarding information by directly uploading Personal Data on the Platform,
    - We will provide the Standard and Premium Employment Services as agreed to be provided in writing.

7. Purpose(s) of the processing (including international transfers) and further processing

- Personal Data is processed and transferred for the following purposes:
    - In relation to Employees, so You can communicate with proposed Employees and in order to onboard them onto the Platform.
    - In relation to Consultants, so You can communicate with proposed Consultants and in order to onboard them onto the Platform.
    - In relation to Employees or Consultants, so that We may fulfil our obligations as employer and to payout salary and other benefits to the Employee or Consultant.
    - In relation to Your authorised users, to authenticate them as authorised users of the Platform and to communicate with them in relation to their use of it.
    - Any other lawful purposes agreed between the parties in writing.

8. The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period

- As set out in section 3 of the DPA. For more detailed information about the retention periods of the Personal Data that We process You can request a copy of our retention policies at: dpo@remote.com.

9. Technical and organisational measures implemented at Remote to ensure information security

- The list of technical and organisational measures implemented at Remote is at Schedule 9.

Schedule 2 - Payroll Services

1. Roles
- We shall act as Processor and You shall act as Controller.

2. Categories of data subjects whose Personal Data is processed

- Payroll Employees registered on Our Platform.

3. Categories of Personal Data processed

- Payment & tax data, Payroll Employees job data, time off data, personal data from powers of attorney.
- personal identification data, address data, administrative data, contract data, feedback data, benefits data, incentives data, working hours data, custom fields data, data in documents, data from expenses, bank account data.
- any other categories of Personal Data You instruct us to collect on Your behalf via the Platform.

4. Sensitive data processed

- Data concerning health, processing of which is necessary for the purpose of carrying out obligations and exercising specific rights of the Controller or data subject in the field of employment.

5. Nature of the processing

Personal Data will be processed as follows:

- authorised users will be appointed by You and invited to the Platform,
- You will onboard Payroll Employees on the Platform,
- Payroll Employees will submit their onboarding information by directly uploading Personal Data on the Platform, and
- in accordance with any additional instructions You may have.

6. Purpose(s) of the processing (including international transfers) and further processing

Personal Data is processed and transferred for the following purposes:

- In relation to Payroll Employees, so You can communicate with proposed Employees and in order to onboard them onto the Platform.
- In relation to Payroll Employees, so that We may fulfil our Payroll Service to the Payroll Employees.

7. The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period

- until the end of the provision of Our Services to You unless otherwise required by applicable law as set out in section 7.9 of this DPA. For more detailed information about the retention periods of the Personal Data that We process You can request a copy of our retention policies at: dpo@remote.com.

1. Technical and organisational measures implemented at Remote to ensure information security

8. The list of technical and organisational measures implemented at Remote is at Schedule 9.

Schedule 3 - Human Resources Information System (HRIS)

1. Roles

- We shall act as Processor and You shall act as Controller in connection with any human resources information system Services we offer via the Platform.

2. Categories of data subjects whose Personal Data is processed

- Your employees registered on Our Platform.

3. Categories of Personal Data processed

- personal identification data, address data, administrative data, emergency person contact details, contract data, time off data, feedback data, employment data, custom fields data, data in documents, data from invoices, bank account data.
- any other categories of Personal Data You instruct us to collect on Your behalf via the Platform.

4. Sensitive data processed

- Data concerning health, processing of which is necessary for the purpose of carrying out obligations and exercising specific rights of the Controller or data subject in the field of employment.

5. Nature of the processing

Personal Data will be processed as follows:

- authorised users will be appointed by You and invited to the Platform,
- You will onboard employees on the Platform,
- Employees will submit their onboarding information by directly uploading Personal Data on the Platform, and
- We will provide the employees Services agreed to be provided in writing.

6. Purpose(s) of the processing (including international transfers) and further processing

Personal Data is processed and transferred for the following purposes:

- In relation to employees, so You can communicate with proposed employees and
- in order to onboard employees onto the Platform.
- In order to provide You any Services which you request

7. The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period

- until the end of the provision of Our Services to You unless otherwise required by applicable law as set out in section 7.9 of this DPA. For more detailed information about the retention periods of the Personal Data that We process You can request a copy of our retention policies at: dpo@remote.com.

8. Technical and organisational measures implemented at Remote to ensure information security.

- The list of technical and organisational measures implemented at Remote is at Schedule 9.

Schedule 4 - Contractor Management Services

1. Roles
- We shall act as Processor and You shall act as Controller in connection with any Contractor Management Services We provide to You.

2. Categories of data subjects whose Personal Data is processed

- Your Contractors registered on Our Platform.

3. Categories of Personal Data processed

- personal identification data, address data, administrative data, emergency person contact details, contract data, feedback data, custom fields data, data in documents, data from invoices, bank account data.
- any other categories of Personal Data You instruct us to collect on Your behalf via the Platform.

4. Sensitive data processed

- Biometric data for the purpose of identity verification of a natural person;

5. Nature of the processing

Personal Data will be processed as follows:

- authorised users will be appointed by You and invited to the Platform,
- You will onboard Contractors on the Platform,
- Contractors will submit their onboarding information by directly uploading Personal Data on the Platform, and
- We will provide the Contractor management Service agreed to be provided in writing.

6. Purpose(s) of the processing (including international transfers) and further processing

Personal Data is processed and transferred for the following purposes:

- In relation to Contractors, so You can communicate with proposed Contractors and in order to onboard them onto the Platform.
- In relation to Contractors, so that We can deliver Contractor Management Services.

7. The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period

- until the end of the provision of Our Service to You unless otherwise required by applicable law as set out in section 7.9 of this DPA. For more detailed information about the retention periods of the Personal Data that We process You can request a copy of our retention policies at: dpo@remote.com.

8. Technical and organisational measures implemented at Remote to ensure information security

- The list of technical and organisational measures implemented at Remote is at Schedule 9.

Schedule 5 - Contractor of Record Services

1. Roles

● Each party acts as an independent Controller in the context of CoR and shall process Personal Data in compliance with applicable Data Protection Laws and these Terms.

2. Categories of data subjects whose Personal Data is processed

● Subcontractors, and

● Authorised users of the Remote Platform engaged by You.

3. Categories of Personal Data processed

● In relation to Subcontractors: personal identification data, address data, contact data, administrative data, emergency person contact data, contract data, feedback data, custom fields data, data in documents, data from invoices, bank account data, device data.

● In relation to Your authorised users: personal identification data, authorised-user-generated access credentials, contact data, device data and the content of communications relating to their use of the Remote platform.

● Any other categories of Personal Data agreed to be processed by the parties in writing and/or required by law.

4. Sensitive data processed

● Biometric data for the purpose of identity verification of a natural person.

5. Nature of the processing

● Personal Data will be processed as follows:

o authorised users will be appointed by You and invited to the Platform,

o You will invite Subcontractors on the Platform,

o Subcontractors will submit their onboarding information by directly uploading Personal Data on the Platform, and

o We will provide the CoR Services as agreed to be provided in writing.

6. Purpose(s) of the processing (including international transfers) and further processing Personal Data is processed and transferred for the following purposes:
- In relation to Subcontractors, so that We may fulfil our obligations to perform our agreements with them and/or for other purposes required by law.
- In relation to Your authorised users, to authenticate them as authorised users of the Platform and to communicate with them in relation to their use of it.
- Any other lawful purposes agreed between the parties in writing.

7. The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period

● As set out in section 3 of the DPA. For more detailed information about the retention periods of the Personal Data that We process You can request a copy of our retention policies at: dpo@remote.com.

8. Technical and organisational measures implemented at Remote to ensure information security

● The list of technical and organisational measures implemented at Remote is at Schedule 9.

Schedule 6 - Perform

1. Roles
● We shall act as Processor and You shall act as Controller in connection with Perform.
2. Categories of data subjects whose Personal Data is processed
● Users appointed by You registered on Our Platform.
3. Categories of Personal Data processed
● personal identification data, performance data, feedback data, other categories of Personal Data uploaded by the appointed users via Perform.
● any other categories of Personal Data You instruct us to collect on Your behalf via Perform.
4. Sensitive data processed
● Any sensitive data uploaded by the appointed users via Perform.
5. Nature of the processing

Personal Data will be processed as follows:

● Users appointed by You will be invited to Perform,
● the appointed users will submit their performance related information including Personal Data by directly uploading it on the Platform via Perform, and
● You will receive access to the submitted performance related information via Perform.
6. Purpose(s) of the processing (including international transfers) and further processing

Personal Data is processed and transferred for the following purposes:

● In relation to the users appointed by You, so that We can deliver Perform to You to streamline Your performance management processes.
7. The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period
● until the end of the provision of Perform to You unless otherwise required by applicable law as set out in section 7.9 of this DPA. For more detailed information about the retention periods of the Personal Data that We process You can request a copy of our retention policies at: dpo@remote.com.
8. Technical and organisational measures implemented at Remote to ensure information security
● The list of technical and organisational measures implemented at Remote is at Schedule 9.

Updated April 30, 2026

Schedule 7 - Mobility as a Service

1. Roles
- We shall act as Processor and You shall act as Controller in connection with the Mobility as a Service we provide to You in connection with the Payroll services and/or Human Resources Information System (HRIS) services we deliver to you.
2. Categories of data subjects whose Personal Data is processed
- Your active employees registered on the Platform or pre-invitation candidates registered on, but not invited to the Platform, appointed by You for mobility assessment.
3. Categories of Personal Data processed
- personal identification data, address data, contact data, administrative data, employment data, data in documents, other categories of Personal Data uploaded by your employees registered on the Platform or pre-invitation candidates appointed for mobility assessment.
- any other categories of Personal Data You instruct us to collect on Your behalf via the Platform.
4. Sensitive data processed
- Any necessary sensitive data uploaded by You, the employees or pre-invitation candidates appointed for mobility assessment.
5. Nature of the processing

Personal Data will be processed as follows:

- **Active Employees:** Your employees invited to the Platform and appointed by You for mobility assessment, shall upload their own necessary Personal Data and supporting documents directly onto the Platform;
- **Pre-invitation Candidates:** Your candidates registered on, but not invited to the Platform, and appointed by You for a pre-invitation mobility assessment, shall have their necessary Personal Data and supporting documents directly uploaded onto the Platform by You;
- We will process their Personal Data necessary for the purpose of the mobility service assessment
- Where necessary, we may engage a third party to help us with the processing and
- You will receive access to our final assessment via the Platform.

6. Purpose(s) of the processing (including international transfers) and further processing

Personal Data is processed and transferred for the following purposes:

- In relation to Your employees registered on the Platform or pre-invitation candidates registered on, but not invited to the Platform, appointed for mobility assessment, so we can process their Personal Data necessary for the purpose of the mobility service assessment.

7. The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period

- until the end of the provision of the Payroll services and/or Human Resources Information System (HRIS) services we deliver to You unless otherwise required by applicable law as set out in section 7.9 of this DPA. For more detailed information about the retention periods of the Personal Data that We process You can request a copy of our retention policies at: dpo@remote.com.

8. Technical and organisational measures implemented at Remote to ensure information security

- The list of technical and organisational measures implemented at Remote is at Schedule 9.

Schedule 8 – Standard Contractual Clauses (International Transfers)

Annex I.

A. List of the Parties

Data Exporter

Exporter:	You
Address:	As set out in these Terms (for Us) or on the Platform (for You)
Contact person's name, position and contact details:	Bird and Bird, Data Protection Officer, dpo.remote@twobirds.com (for Us) or as set out on the Platform (for You)
Activities relevant to the data transferred under these Clauses:	As described under Purpose of Processing in Schedules 1-7 of this DPA
Signature and date	As set out in these Terms
Role (controller/processors)	As described under Roles in Schedules 1-7 of this DPA

Data Importer

Importer	Remote

Address	As set out in these Terms (for Us) or on the Platform (for You)
Contact person:	Bird and Bird, Data Protection Officer, dpo.remote@twobirds.com (for Us) or as set out on the Platform (for You)
Activities relevant to the data transferred under these Clauses:	As described under Purpose of Processing in Schedules 1-7 to this DPA (as applicable to the Service(s) for which You engage Us)
Signature and date	As set out in these Terms
Role (controller/processors)	As described under Roles in Schedules 1-7 of this DPA.

B. Description of Transfer (for both modules)

- As set out in section 6 of the DPA and in the applicable Schedules 1-7 to this DPA.

C. Competent Authority (for both modules)

- The Dutch data protection authority.

Annex II. Technical And Organisational Measures Including Technical And Organisational Measures To Ensure The Security Of The Data

- As set out in the Schedule 9 of the DPA.

Schedule 9 - Technical and Organisational Measures

Technical and organisational measures at Remote implemented to ensure information security including relevant certifications are available to check at https://trust.remote.com.

Digital Operational Resilience Act (DORA). To the extent You are an entity falling under the scope of Digital Operational Resilience Act (REGULATION (EU) 2022/2554) and Remote is considered an ICT (Information and Communication Technology) third party service provider, Remote's DORA Addendum available at trust.remote.com shall apply to Our provision of Services to You. For the purposes of the DORA Addendum, the parties assume Remote is not supporting Your important or critical business functions.

We have implemented the following technical and organisational measures in order to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

- data encryption in transit,
- data encryption at rest,
- architecture network isolation through private networks,
- fully auditable access and changes,
- all systems protected by a firewall with security threat detection and prevention mechanisms,
- least privilege principle limiting systems' access to essential personnel only,
- all internal tools and systems require SSO,
- the practice of continuous credentials auditing and management,
- the conducting of internal security and privacy training,
- infrastructure-as-code allowing for quick rebuilding and portability,
- continuous monitoring of applications and infrastructure,
- regular data backups,
- applicational logs stored off site and kept for a limited period of time, and
- the processing involves solely such data that is strictly necessary for business operations.
- To the extent such processing concerns sensitive data the following safeguards that fully take into consideration the nature of the data and the risks involved are applied: strict purpose limitation; access restriction; data encryption in transit and data encryption at rest.