**Data Processing Addendum**

**Last Updated: 14 April 2025**
**Effective: 14 April 2025**

# DATA PROCESSING ADDENDUM

1 PURPOSE ..... 3
2 DEFINITIONS ..... 3
3 CONTRACTUAL DOCUMENTS ..... 4
4 DURATION OF THE ASSIGNMENT/NOTICE OF TERMINATION ..... 4
5 RELATIONSHIP OF THE PARTIES ..... 4
6 CONTROLLER TO CONTROLLER CLAUSES ..... 5
7 CONTROLLER TO PROCESSOR CLAUSES ..... 5
8 TECHNICAL AND ORGANISATIONAL MEASURES ..... 7
9 CROSS-BORDER DATA TRANSFERS ..... 7
10 LIABILITY ..... 8
11 FINAL PROVISIONS ..... 8
APPENDIX 1: PERSONAL DATA ..... 9
1 PERSONAL DATA SERVICE PROVIDER PROCESSES AS CONTROLLER (DEEL LOCAL PAYROLL APPLICATION) ..... 9
2 PERSONAL DATA SERVICE PROVIDER PROCESSES AS PROCESSOR (SERVICE: SOFTWARE AS A SERVICE, PAYROLL OUTSOURCING): ..... 9
APPENDIX 2: TECHNICAL AND OPERATIONAL MEASURES ..... 12
1 INTRODUCTION ..... 12
2 ADMISSION CONTROL ..... 12
3 ACCESS CONTROL ..... 12
4 ACCESS MONITORING ..... 12
5 TRANSFER CONTROL ..... 13
6 INPUT CONTROL ..... 13
7 ORDER CONTROL ..... 13
8 AVAILABILITY CONTROL ..... 13
9 SEPARATION CONTROL ..... 14
10 PROCEDURES FOR PERIODIC REVIEW AND EVALUATION ..... 14
APPENDIX 3: CONTACT DETAIL OF THE PARTIES ..... 15
1 AUTHISED REPRESENTATIVES OF THE PARTIES ON DATA PROTECTION MATTERS ..... 15
APPENDIX 4: STANDARD CONTRACTUAL CLAUSES – ANNEX 1: PERSONAL DATA ..... 16
1 LIST OF PARTIES ..... 16
APPENDIX 5: SUB-PROCESSORS ..... 18
1 SUB-PROCESSORS ..... 18
APPENDIX 6: JURISDICTION SPECIFIC TERMS ..... 19
1 AUSTRALIA ..... 19
2 BOTSWANA ..... 19
3 BRAZIL ..... 19
4 CANADA ..... 19
5 EUROPEAN ECONOMIC AREA (EEA) ..... 19
6 ISRAEL ..... 19
7 JAPAN ..... 19

8 KENYA ..... 19
9 MEXICO ..... 19
10 NIGERIA ..... 19
11 SINGAPORE ..... 19
12 SOUTH AFRICA ..... 20
13 SWITZERLAND ..... 20
14 UNITED KINGDOM (UK) ..... 20
15 UNITED STATES OF AMERICA ..... 20
16 CHINA ..... 20
17 HONG KONG ..... 20
APPENDIX 7: RETENTION AND / OR DELETION OF PERSONAL DATA ..... 21
1 PROCESS FOR OBTAINING DATA AT END OF CONTRACT PERIOD ..... 21
2 DELETION OF PERSONAL DATA ..... 21
3 VALUE ADDED HISTORICAL INFORMATION SERVICE ..... 21
4 GENERAL ..... 21

**Data Processing Addendum**

**1 PURPOSE**

1.1 Service Provider and Customer have entered into the Agreement for the provision of services. This Data Processing Addendum (hereinafter "DPA" or "Addendum") and its applicable DPA Appendixes apply to the processing of Personal Data by the Parties subject to the Data Protection Laws in order to provide services ("Services") pursuant to the Agreement between Service Provider and Customer.

1.2 To provide the Services in accordance with the Agreement, Service Provider processes Personal Data as described in Appendix 1.

1.3 As part of their contractual relations, the Parties shall undertake to comply with the applicable Data Protection Laws with respect to the processing of Personal Data covered under this DPA.

**2 DEFINITIONS**

2.1 "**Controller**", depending on the Applicable Data Protection Law and means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; where the purposes and means of such processing are determined by Applicable Data Protection Law, Customer or the specific criteria for its nomination may be provided for by Applicable Data Protection Law.

2.2 "**Data Protection Law/s**" means all data protection laws and regulations applicable to a party's processing of a Customer's Personal Data under the Agreement, including, where applicable, EU/UK Data Protection Laws, Non-EU Data Protection Laws, and any other applicable data protection laws.

2.3 "**EU/UK Data Protection Laws**" means:

2.3.1 Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "EU GDPR");

2.3.2 the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR");

2.3.3 the EU e-Privacy Directive (Directive 2002/58/EC). and;

2.3.4 any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of clause 1.22.1, clause 1.22.2 and clause 1.22.3, in each case as may be amended or superseded from time to time.

2.4 "**Non-EU Data Protection Laws**" means any other applicable laws to the processing of Customer's Personal Data, including without limitation the applicable data protection laws described in Appendix 6 (Jurisdiction Specific Terms).

2.5 "**Personal Data**", depending on the Applicable Data Protection Law and means any information relating to a Data Subject.

2.6 "**Processor**" depending on the Applicable Data Protection Law and means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of Customer in terms of a contract or mandate, without coming under the direct authority of that party.

2.7 "**Restricted Transfer**" means:

2.7.1 where the EU GDPR applies, a transfer of personal data from the European Economic Area or Switzerland to a country outside of the European Economic Area or Switzerland which is not subject to an adequacy determination by the European Commission. and;

2.7.2 where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

2.8 "**Standard Contractual Clauses**" means where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs"). The Standard Contractual Clauses shall be incorporated by reference and form an integral part of the Data Processing Addendum.

2.9 "**Sub-Processor**" means a sub-contractor appointed by the Service Provider to process the Personal Data.

2.10 "**UK Addendum**" means the addendum to the Standard Contractual Clauses issued by the UK Information Commissioner under Section 119A(1) of the UK Data Protection Act 2018 (version B1.0, in force March 21, 2022). The UK Addendum shall be incorporated by reference and form an integral part of the Data Processing Addendum.

**3 CONTRACTUAL DOCUMENTS**

3.1 This DPA and its Appendixes constitute the entire Data Processing Addendum between the Parties for the provision of the services pursuant to the Agreement. It replaces all previous agreements relating to its object.

3.2 Some of the contractual documents may be amended or enriched during the fulfilment of the Addendum. In any event, these amendments or enrichments must be covered by an amendment signed by the Parties. No modifications may be made to the Addendum and its Appendixes without a document signed by both Parties.

**4 DURATION OF THE ASSIGNMENT/NOTICE OF TERMINATION**

4.1 The duration of the assignment (term of the DPA) is coextensive with the term of this Agreement.

4.2 The termination of this Addendum therefore depends on the provisions concerning the duration and the termination of this Agreement. Termination of this Agreement shall also have the effect of terminating this DPA.

4.3 Furthermore, the premature termination of this Addendum upon written notice to the other Party shall be permissible in the event of such other Party's serious breach of statutory or contractual data protection provisions under the Data Protection Laws, insofar as the contracting Party in question cannot reasonably be expected to continue this DPA.

4.4 The parties acknowledge that the termination of the DPA at any time and for any reason does not exempt them from their obligations under the Data Protection Laws relating to the collection, processing, and use of Personal Data.

**5 RELATIONSHIP OF THE PARTIES**

5.1 Service Provider will process the Personal Data as Controller for the purposes to the extent relevant to the Services in order to:

5.1.1 manage the relationship with Customer

5.1.2 where applicable, carry out Service Provider's Affiliates core business operations, such as:

5.1.2.1 accounting and filing taxes;

5.1.2.2 detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the Services. and;

5.1.2.3 0erform identity verification;

5.1.3 comply with Service Provider's legal or regulatory obligations. and;

5.1.1 as otherwise permitted under Data Protection Laws and in accordance with this Addendum, the Agreement, and the Service Provider's Affiliate Privacy Policy, which can be found at https://www.payspace.com/privacy-policy;

5.2 The parties acknowledge and agree that each is acting independently as a Controller with respect to Personal Data and the parties are not joint controllers. Service Provider will process the Personal Data in accordance as Controller as set forth in clause 6.

5.3 Where Service Provider processes the Personal Data in the performance of the Services, Service Provider acts as Customer's Processor only where Customer determines the purpose and means of the processing. In such circumstances, Service Provider will process the Personal Data in accordance with Customer's instructions, as Controller, to Service Provider, as Processor, as set forth in clause 7.

5.4 Customer acknowledges that in the provision of Service Provider Integrations (as listed in Appendix 1), Service Provider acts as a Processor and may, on receipt of instructions from Customer, transfer Personal Data to and otherwise interact with third parties. Customer agrees that if and to the extent such transfers occur, Customer is responsible for entering into separate contractual arrangements with such third parties requiring them to comply with obligations in accordance with the Applicable Data Protection Laws. For the avoidance of doubt, Dee Integrations are optional add-ons to the services listed in Appendix 1. Such third parties are not sub-processors of Service Provider in the context of this Addendum and Service Provider is not a party to the arrangements between the Customer and the third party.

**Data Processing Addendum**

## 6 CONTROLLER TO CONTROLLER CLAUSES

6.1 In respect of the Personal Data processed by the Parties acting as a Controller under this Addendum, each Party will:

6.1.1 ensure that the persons engaged in the processing of Personal Data are bound by appropriate confidentiality obligations;

6.1.2 comply promptly with any lawful request from the other Party requesting access to, copies of, or the amendment, transfer, or deletion of the Personal Data to the extent the same is necessary to allow either Party to fulfill its obligations under the Data Protection Laws;

6.1.3 notify the other Party within forty-eight (48) hours if it receives any complaint, notice, or communication (whether from a data subject, competent supervisory authority, or otherwise) relating to the processing of Personal Data or to either Party's compliance with Data Protection Laws under this Addendum, and provide the other Party with reasonable cooperation, information and assistance in relation to any such complaint, notice or communication;

6.1.4 notify the other Party immediately if it becomes aware of a breach of this clause, in which case the Party in breach shall take any and all steps to remedy such breach;

6.1.5 facilitate the handling of any Personal Data Breach, that is likely to result in a risk to the rights and freedoms of natural persons for which the other Party is responsible as soon as reasonably practicable upon becoming aware, which shall include the Party responsible for the breach notifying the relevant supervisory authority, promptly and in any event no later than seventy-two (72) hours after becoming aware of it, as well as the relevant data subjects without undue delay, where required by the Data Protection Laws;

6.1.6 provide reasonable assistance in fulfilling the other Party's obligations under the Data Protection Laws. and;

6.1.7 both Parties may engage with third parties in connection with the Services and agree to comply with the applicable requirements under Data Protection Laws in relation to third parties. Both parties shall be liable for the acts and omissions of their respective third parties to the same extent such parties would be liable under the terms of this DPA, except as otherwise set forth in the Agreement.

## 7 CONTROLLER TO PROCESSOR CLAUSES

7.1 In respect of the Personal Data processed by Service Provider as a Processor acting on behalf of Customer under this Addendum, the Processor will:

7.1.1 process the Personal Data only on Customer's written instructions, unless required by law to process it differently (in which case it shall, if permitted by such law, promptly notify Customer of that requirement before processing);

7.1.2 process the Personal Data only to the extent, and in such a manner, as is necessary for the purposes of carrying out its obligations under the Agreement;

7.1.3 ensure that persons engaged in the processing of Personal Data are bound by appropriate confidentiality obligations and have undergone privacy and security training;

7.1.4 keep a record of the processing it carries out, and ensure the same is accurate;

7.1.5 comply promptly with any lawful request from Customer requesting access to, copies of, or the amendment, transfer or deletion of the Personal Data to the extent the same is necessary to allow Customer to fulfil its own obligations under the Data Protection Laws, including Customer's obligations arising in respect of a request from a data subject;

7.1.6 notify Customer promptly if it receives any complaint, notice or communication (whether from a data subject, competent supervisory authority or otherwise) relating to the processing, the Personal Data or to either party's compliance with the Data Protection Laws as it relates to this Addendum, and provide Customer with reasonable co-operation, information and other assistance in relation to any such complaint, notice or communication;

7.1.7 ensure in each case that, prior to the processing of any Personal Data by any Sub-Processor, the Processor and the Sub-Processor agree to contract on the terms set out in this Data Protection Addendum ("Relevant Terms"). The Processor shall procure the performance of the Relevant Terms by the Sub-Processor and shall be directly liable to the Customer for any breach by the Sub-Processor of any of the Relevant Terms;

7.1.8 only transfer the Personal Data outside of the European Economic Area if it has fulfilled each of the following conditions:

7.1.8.1 it has in place any of the specifically approved safeguards for data transfers (as recognized under the Data Protection Laws) in relation to the transfer;

7.1.8.2 data subjects continue to have enforceable rights and effective legal remedies following the transfer;

7.1.8.3 it provides an adequate level of protection to any Personal Data that is transferred (including by way of a European Commission finding of adequacy). and;

7.1.8.4 It complies with reasonable instructions with respect to the transfer;

7.1.9 inform Customer without undue delay within forty-eight (48) hours after having become aware of a breach if any Personal Data processed under this Addendum is lost or destroyed or becomes damaged, corrupted, or unusable or is otherwise subject to unauthorized or unlawful processing including unauthorized or unlawful access or disclosure ("Personal Data Breach");

7.1.10 promptly provide Customer with full cooperation and assistance in respect of the Personal Data Breach and all information in the Processor's possession concerning the Personal Data Breach, including the following:

7.1.10.1 the possible cause and consequences of the Personal Data Breach;

7.1.10.2 the categories of Personal Data and the approximate number of data subjects involved; and

7.1.10.3 the measures taken by the Processor to mitigate any damage;

7.1.10.4 inform Customer promptly if it receives a request from a data subject exercising their data subject rights and provide Customer with reasonable cooperation and assistance in relation to such request;

7.1.11 not disclose the Personal Data to any third party other than at the request of Customer or as otherwise required under the Agreement;

7.1.12 provide reasonable assistance to the Customer in complying with its obligations under Data Protection Laws with respect to security, breach notifications, data protection impact assessments, and consultations with supervisory authorities or regulators;

7.1.13 provide Customer with all information that is necessary to enable Customer to monitor the Processor's compliance with the Data Protection Laws and its obligations under this Addendum at any time during regular business hours. Service Provider may satisfy Customer's right of audit under the Data Protection Laws in relation to Personal Data, by providing an audit report not older than eighteen (18) months, prepared by an independent external auditor demonstrating that Service Provider's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard. Service Provider reserves the right to refuse audit requests from an entity that is a competitor of Service Provider.; and

7.1.14 delete or return that Personal Data to Customer at the end of the duration of the processing, and at that time delete or destroy existing copies. If return or destruction is impracticable or prohibited by law, rule, or regulation, Service Provider shall take measures to block such Personal Data from any further processing (except to the extent necessary for processing required by law, rule, or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control.

7.1.15 Customer acknowledges and agrees that Service Provider may:

7.1.15.1 engage its Affiliates and Sub-Processors listed in **Appendix 5** to this Addendum to access and process Personal Data in connection with the Services. and;

7.1.15.2 from time to time engage additional third parties for the purpose of providing the Services, including without limitation the processing of Personal Data. By way of this Addendum, Customer provides general written authorization to Service Provider to engage Sub-Processors as necessary to perform the Services.

7.1.16 A list of Service Provider's current Sub-Processors (the "List") is available to Customer, on the Service Provider platform. Such a List may be updated by Service Provider from time to time. Service Provider provides a mechanism to subscribe to notifications of new Sub-Processors and Customer agrees to subscribe to such notifications where available. For instructions on how to subscribe to the notification mechanism, please follow the steps in **Appendix 5**. At least ten (10) days before enabling any third party other than existing Sub-Processors to access or participate in the processing of Personal Data, Service Provider will add such third parties to the List and notify Customer. The Customer may object to such an engagement by informing Service Provider within ten (10) days of receipt of the aforementioned notice by Service Provider, provided such

objection is in writing and based on reasonable grounds relating to data protection. Customer acknowledges that certain Sub-Processors are essential to providing the Services and that objecting to the use of a Sub-Processor may prevent Service Provider from offering the Services to Customer.

7.1.17 If Customer reasonably objects to an engagement in accordance with Section 7, and Service Provider cannot provide a commercially reasonable alternative within a reasonable period of time, Customer may discontinue the use of the affected Service by providing written notice to Service Provider. Discontinuation shall not relieve Customer of any fees owed to Service Provider under the Agreement.

If Customer does not object to the engagement of a third party in accordance with Section 7 within ten (10) days of notice by Service Provider, that third party will be deemed a Customer - approved Sub-Processor for the purposes of this Addendum.

7.1.18 Service Provider will enter into a written agreement with the Sub-Processor imposing on the Sub-Processor data protection obligations comparable to those imposed on Service Provider under this Addendum with respect to the protection of Personal Data. In case a Sub-Processor fails to fulfill its data protection obligations under such written agreement with Service Provider, Service Provider will remain liable to Customer for the performance of the Sub-Processor's obligations under such agreement.

## 8 TECHNICAL AND ORGANISATIONAL MEASURES

8.1 Service Provider shall take suitable technical and organizational measures appropriate to the risk to ensure for protection of the security, confidentiality, and integrity of the Personal Data it processes under this DPA. Service Provider guarantees that it has carried out the technical and organizational measures specified in Appendix 2 to this DPA.

8.2 The technical and organizational measures are subject to the current state of technology and technical progress. In this regard, Service Provider is permitted to implement adequate alternative measures, provided that these measures may not provide a lower level of security to Customer data than the stipulated measures in Appendix 2 to this DPA.

## 9 CROSS-BORDER DATA TRANSFERS

9.1 The parties agree that when the transfer of Personal Data is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses or the UK Addendum.

9.1.1 In relation to Personal Data that is protected by the EU GDPR and Restricted Transfers outside the EU, the Standard Contractual Clauses shall be incorporated into this Addendum by reference and the information required to complete the Standard Contractual Clauses is as follows:

9.1.1.1 Module One (Controller to Controller) will apply where both Customer and Service Provider are Controllers of the Personal Data under this DPA;

9.1.1.2 Module Two (Controller to Processor) will apply where Customer is a Controller and Service Provider is a Processor of the Personal Data under this DPA;

9.1.1.3 in Clause 7, the optional docking clause will apply;

9.1.1.4 in Clause 9, Option 2 applies to the use of sub-processors;

9.1.1.5 in Clause 11, the optional language will not apply;

9.1.1.6 Clause 13(a) Option 1 applies (supervisory authority with responsibility for ensuring compliance by the data exporter shall act as competent supervisory authority) as indicated in Appendix 4.

9.1.1.7 in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law of The Republic of Ireland;

9.1.1.8 in Clause 18(b), disputes shall be resolved before the courts of The Republic of Ireland;

9.1.1.9 Annex I of the EU SCCs shall be deemed completed with the information set out in **Appendix 4** to this DPA; and

9.1.1.10 Annex II of the EU SCCs shall be deemed completed with the information set out in **Appendix 2** to this DPA.

9.1.2 In relation to Personal Data that is protected by the UK GDPR and Restricted Transfers out of the UK, the UK Addendum shall be incorporated into this Addendum by reference and the information required to complete the UK Addendum is as follows:

9.1.2.1 Part 1 of the UK Addendum is completed as follows:

a. in Table 1, as set forth in **Appendix 4.A** "List of parties**"** and **Appendix 3** 'Contact details of the parties';

b. in Table 2, the second option is selected, and the "Approved EU SCCs" are the Standard Contractual Clauses referred to in Section 11.1 (a) of this section;

c. in Table 3, Annexes 1 (A and B) of the "Approved EU SCCs" are **Appendix 4** (A and B) to this DPA, and Annex II of the "Approved EU SCCs" is **Appendix 2** to this DPA; and

d. in Table 4, both the "Importer" and the "Exporter" can terminate the UK Addendum.

9.1.2.2 Part 2 of the UK Addendum is completed with the Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

9.1.3 In relation to Personal Data that is protected by the Swiss DPA, the EU SCCs will apply completed as follows:

9.1.3.1 references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;

9.1.3.2 references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA;

9.1.3.3 references to "EU", "Union" and "Member State law" shall be replaced with "Switzerland";

9.1.3.4 Clause 13(a) and Part C of Annex II shall be deleted;

9.1.3.5 references to the "competent supervisory authority" and "competent courts" shall be replaced with "the Swiss Federal Data Protection and Information Commissioner" and "relevant courts in Switzerland";

9.1.3.6 Clause 17 shall be replaced to state "The Clauses are governed by the laws of Switzerland"; and

9.1.3.7 Clause 18 shall be replaced to state "Any dispute arising from these Clauses shall be resolved by the applicable courts of Switzerland. The Parties agree to submit themselves to the jurisdiction of such courts".

9.1.4 In the event that any provision of this Addendum contradicts, directly or indirectly, the Standard Contractual Clauses or the UK Addendum, the Standard Contractual Clauses and the UK Addendum shall prevail. Where PIPL applies, the parties agree that the PIPL SCCs ("个人信息出境标准合同") shall prevail over any other data protection agreement.

9.1.5 If the Standard Contractual Clauses or the UK Addendum are deemed invalid by a governmental entity with jurisdiction over transferred personal data (e.g., the EU Court of Justice or the UK Government) or if such governmental entity imposes additional rules and/or restrictions regarding such Transferred Personal Data, the parties agree to work in good faith to find an alternative and/or modified approach with respect to such Transferred Personal Data which is in compliance with applicable laws.

## 10 LIABILITY

10.1 This Addendum is without prejudice to the rights and obligations of the Parties under the Agreement which shall continue to have full force and effect, including any limitations and exclusions on liability contained therein which shall apply to this Addendum as if fully set forth herein.

## 11 FINAL PROVISIONS

11.1 If individual provisions of this Addendum should be or become ineffective, this shall not affect its remaining provisions. The Parties undertake to replace the ineffective provisions with a legally valid provision that comes closest to the purpose of the ineffective provisions.

11.2 In the event of contradictions between this Addendum and any other agreements between the Parties, especially the Agreement, the provisions of this Addendum shall take precedence.

11.3 Ancillary agreements, amendments, and additions to this Addendum must be made in writing. This also applies to the amendment of this requirement for written form.

**Data Processing Addendum – Appendix 1: Personal Data**

**APPENDIX 1: PERSONAL DATA**

**1 PERSONAL DATA SERVICE PROVIDER PROCESSES AS CONTROLLER (DEEL LOCAL PAYROLL APPLICATION)**

1.1 Categories of data Subjects. The personal data transferred concern the following categories of data Subjects:

1.1.1 Customer's Corporate Data, Customer's representatives and Customer 's authorized users

1.2 Categories of Personal Data. The personal data transferred concern the following categories of data:

1.2.1 Contact information: full name, e-mail addresses, phone numbers, and other ways in which Service Provider can contact the data subject

1.2.2 Communications: any communication Customer has with Service Provider, like emails and phone calls

1.2.3 Information regarding the usage of the Service Provider Platform, like payment transactions and technical connection data (IP address, location, logs, etc.)

1.2.4 Identification information: LinkedIn profile URL, government ID/passport, and other information to allow Service Provider to perform Know Your Business checks.

1.3 Sensitive Categories: The personal data transferred concern the following special categories of data:

1.3.1 Any personal data that may appear on identification documentation and are defined as special categories of data under applicable data protection laws (e.g. religion, government ID number).

1.4 Processing operations. The personal data transferred will be processed in accordance with the Agreement and may be subject to the following processing activities:

1.4.1 storage and other processing necessary to provide, maintain, and update the Service Provider Platform Services provided to the Customer

1.4.2 to provide technical support to the Customer

1.4.3 disclosures in accordance with the Agreement, as compelled by law

1.5 Duration of processing. Service Provider will process personal data as a controller for as long as needed to provide the Services under the Agreement or as required by law.

**2 PERSONAL DATA SERVICE PROVIDER PROCESSES AS PROCESSOR (SERVICE: SOFTWARE AS A SERVICE, PAYROLL OUTSOURCING):**

2.1 Categories of data subjects. The personal data transferred concern the following categories of data subjects:

2.1.1 Customer s direct employees and contractors

2.2 Categories of personal data. The personal data transferred concern the following categories of data:

2.2.1 Identification information: name, addresses, e-mail addresses, phone numbers, number of personal ID card, date of issuance, issued by, date of birth, and PIN (Personal Identification Number), respectively tax ID number and/or personal number of a foreigner

2.2.2 Sex

2.2.3 Family status and information about dependent persons (children), when necessary

2.2.4 Bank account information

2.2.5 Tax status information

2.2.6 Employment information: labour remuneration, annual leave and other types of leave, as well as the grounds for such, pension, compensations, bonuses and other benefits, date of employment, period of employment, labour agreement terms, and information about termination of labour relationship, place of work, information about the job (including job positions,

job descriptions, employment history, working time, information about company email), details on current and previous remuneration(s)

2.2.7 Information about distraints over labour relationships and related information

2.2.8 Other information about the persons in their respective capacities, which might be necessary with respect to the assigned work

2.3 Sensitive Categories. The personal data transferred concern the following special categories of data:

2.3.1 Information about the health status of the employees (e.g. sick leaves, medical certificates)

2.3.2 A copy of the ID document/in all cases when this is required by law

2.4 Processing operations. The personal data transferred will be processed in accordance with the Agreement and may be subject to the following processing activities:

2.4.1 Registration of labour agreements (new hires), terminations, and changes in labour relationships, according to the requirements of the applicable legislation

2.4.2 Payroll gross-to-net calculation for the employees, which contains the settlement of the basic salary, bonuses, social expenses, assignment fees, holidays, and sick benefits, etc., including deductions (e.g. alimony, credit deductions, etc.) by the written instructions of the employer

2.4.3 Determination of the taxes and contributions related to salary/remunerations

2.4.4 Preparation of summary reports for the employer, which contain the gross and net salaries per employee, and taxes and contributions paid by the employees and the employer (payroll ledger)

2.4.5 Preparation and sending of the pay slips.

2.4.6 Preparation of electronic bank transfer files for the payables to tax authorities with deadlines, amounts, and bank account numbers; as well as employees' net salaries, and entering payment orders in e-banking platforms;

2.4.7 Preparation of General ledger file in electronic format for the purposes of accounting processing (accrual) of salaries/remunerations, compensations, insurances, taxes on incomes of individuals, etc. (recapitulation).

2.4.8 Preparation and submission via the Internet of employment declarations, as well as declarations and other documents in relation to sick leaves, motherhood and other similar in accordance with the applicable legislation

2.4.9 Preparation of employment certificates (salary notes) for employees, when necessary, based on a requirement of law, or in case of a request from the employees

2.4.10 Filling-in and preparation of labour books

2.4.11 Preparation of reports for salaries for the annual financial statements

2.4.12 Preparation of annual (and quarterly, if applicable) reports

2.4.13 Submission of sick leave sheets and other documents, related to payments of compensation, provided by the employer

2.4.14 Preparation of labour agreements and addendums, termination orders and other documents, related to initiating, changes and termination of labour employment

2.4.15 Preparation of various reports about salary expenses and elements of the labour remuneration, information for leaves and other similar, upon request by the employer, in case of external independent audit and/or in case of audits by the relevant authorities based on the applicable social, tax and labour legislation

2.4.16 Submission of labour files, payroll ledger and other information to NII in relation to the liquidation of the company of the employer, according to the applicable legislation (if explicitly assigned by the Assignor)

2.4.17 Reporting for statistical and fraud prevention purposes

**Data Processing Addendum – Appendix 1: Personal Data**

2.4.18 Other processing activities, which can be assigned by the Customer to Service Provider under the Agreement

2.5 Duration of processing. Service Provider will process personal data as a processor for the duration outlined in clause 7 of this DPA.

**Data Processing Addendum – Appendix 2: Technical and Operational Measures**

## APPENDIX 2: TECHNICAL AND OPERATIONAL MEASURES

### 1 INTRODUCTION

1.1 Service Provider has implemented comprehensive organizational and technological measures to ensure the safety of personal data as well as undisturbed operation in an optimal manner. The technical and organizational measures listed in this Appendix have been taken.

### 2 ADMISSION CONTROL

2.1 Measures to prevent unauthorized persons from gaining access to the data processing equipment used to process personal data.

| Implemented | Measure |
|---|---|
| Y | Access control guidelines and regulations |
| Y | Security areas are clearly defined |
| Y | Appropriate implementation of measures to secure Datacenter Access |
| Y | Security also outside working hours by alarm system and/or plant security |
| Y | Access only for authorized persons (company employees and external persons) |
| Y | Regulation for external parties |
| Y | Implementation of locks |
| Y | External staff is accompanied by Service Provider staff |

### 3 ACCESS CONTROL

3.1 Measures and procedures to prevent unauthorized persons from using the data processing equipment.

| Implemented | Measure |
|---|---|
| Y | Regulation of user authorizations (administration incl. assignment of rights, assignment of special rights, revocation of authorizations, regular reviews). |
| Y | Password policy (secure passwords, regular changes, regular reviews). |
| Y | Use of encryption routines for mobile data carriers (incl. notebooks, USB sticks) |
| Y | Remote user authentication (cryptographic techniques, hardware identification, VPN solutions) |
| Y | BYOD policy |
| Y | Obligation to maintain data secrecy in accordance with Art. 28 Para. 3 lit. b EU GDPR |
| Y | Role-based authorization |
| Y | Controlled destruction of data carriers |
| Y | Regular security audit |

### 4 ACCESS MONITORING

4.1 Measures to ensure that those authorized for data processing can only access the personal data subject to their access authorization.

| Implemented | Measure |
|---|---|
| Y | Control of access authorization (differentiated authorizations via profiles, roles, time limit) |
| Y | Provision of appropriate authentication technologies |
| Y | Security Logs (ex: unsuccessful and successful authentication attempts). |
| Y | Guidelines for the pseudonymization/anonymization of personal data |

**Data Processing Addendum – Appendix 2: Technical and Operational Measures**

## 5 TRANSFER CONTROL

5.1 Measures to ensure that personal data cannot be read, copied, altered, or removed without authorisation during electronic transmission, transport, or storage on data carriers.

| Implemented | Measure |
|---|---|
| Y | Guidelines for the exchange of information of all kinds |
| Y | Encryption during data transmission and at rest (network encryption, TLS) |
| Y | Logging during the transmission of data |
| Y | Method for detecting and protecting malware |
| Y | Access control |
| Y | Encryption of data carriers before transport |
| Y | Handover of data carriers to authorized persons only |
| Y | Controlled destruction of data carriers |

## 6 INPUT CONTROL

6.1 Measures to ensure authenticated entry of personal data.

| Implemented | Measure |
|---|---|
| Y | Access control |
| Y | Data security policy |
| Y | Process, program and workflow organization |

## 7 ORDER CONTROL

7.1 Measures to ensure that personal data is processed within the boundaries and conditions as set out in this Addendum

| Implemented | Measure |
|---|---|
| Y | Contract in writing with determination of the data protection agreements |
| Y | Formalized order placement |
| Y | Careful selection of the subcontractor |
| Y | Monitoring the proper execution of the contract |
| Y | Separation of duty |

## 8 AVAILABILITY CONTROL

8.1 Measures to ensure that personal data is protected against accidental destruction or loss.

| Implemented | Measure |
|---|---|
| Y | Controlled process to ensure business operations (BCM)/IT-SCM |
| Y | Contingency plans |
| Y | Regular back-ups according to a backup plan |
| Y | Protection of systems against database failure, service level agreements with IT service providers |
| Y | Mirroring of data |
| Y | Antivirus/Firewall |
| Y | Redundant hardware |

**Data Processing Addendum – Appendix 2: Technical and Operational Measures**

## 9 SEPARATION CONTROL

9.1 Measures to ensure that data collected for different purposes can be processed separately.

| Implemented | Measure |
|---|---|
| Y | Customer separation |
| Y | Functional separations |

## 10 PROCEDURES FOR PERIODIC REVIEW AND EVALUATION

10.1 Procedures for regular review, evaluation, and evaluation of the effectiveness of technical and organizational measures

| Implemented | Measure |
|---|---|
| Y | Data Protection Management |
| Y | Incident response management |

## APPENDIX 3: CONTACT DETAIL OF THE PARTIES

### 1 AUTHISED REPRESENTATIVES OF THE PARTIES ON DATA PROTECTION MATTERS

1.1 Service Provider's Privacy team & DPO:

| Name | Email/ Telephone |
|---|---|
| Privacy team & Service Provider DPO | dpo@deel.com |

1.2 Customer's Privacy Representative (if applicable)

| Name | Email / Telephone |
|---|---|
| The Customer's representative will be the officer designated by the Customer from time to time. | The Customer representative's detail will those of the officer designated by the Customer from time to time. |

**APPENDIX 4: STANDARD CONTRACTUAL CLAUSES – ANNEX 1: PERSONAL DATA**

**1 LIST OF PARTIES**

1.1 Controller / Data exporter:

| | |
|---|---|
| Name: | As detailed in Customer details on page 1. |
| Address: | As detailed in Customer details on page 1. |
| Contact person's name, position, and contact details: | As detailed in Appendix 3. |
| Activities relevant to the Data transferred under these Clauses: | Processing of Personal Data necessary to provide the services pursuant to the terms of the Agreement. |
| Signature and date: | This Annex 1 shall be deemed executed upon execution of the DPA. |
| Role (controller/processor): | Controller |

1.2 Controller or Processor / Data importer:

| | |
|---|---|
| Name: | Service Provider Inc. |
| Address: | As detailed in Service Provider details on page 1. |
| Contact person's name, position, and contact details: | As detailed in Appendix 3. |
| Activities relevant to the data transferred under these Clauses: | The provision of international HR services, and related services. |
| Signature and date: | This Annex 1 shall be deemed executed upon execution of the DPA Amendment. |
| Role (controller/processor): | Controller / Processor (as detailed in Appendix 1) |

1.3 Description Of Transfer

| | |
|---|---|
| Categories of data subjects whose personal data is transferred: | As detailed in Appendix 1 |
| Categories of personal data transferred: | As detailed in Appendix 1. |

**Data Processing Addendum – Appendix 4: Standard Contractual Clauses – ANNEX 1: Personal Data**

| | |
|---|---|
| Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: | Sensitive data is transferred as detailed in Appendix 1. Personal Data including sensitive Personal Data will be protected in accordance with Appendix 2. |
| The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): | Continuous for the duration of the Services. |
| Nature of the processing: | Processing of Personal Data to provide services pursuant to the terms of the Agreement, including international payroll services. |
| Purpose(s) of the data transfer and further processing: | Processing operations detailed in Appendix 1 |
| The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: | For the duration of the Services. Upon termination or expiry of the Services, Service Provider shall promptly delete any Personal Data it has processed for Customer in connection with the Services unless Service Provider is required to keep the data for legal and regulatory reasons. |
| For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing: | N/A |

1.4 Competent Supervisory Authority

| | |
|---|---|
| Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs) | Where the EU GDPR applies, the competent authority shall be determined in accordance with Clause 13 of the Standard Contractual Clauses.<br><br>Where the UK GDPR applies, the competent authority shall be the UK Information Commissioner's Office. |

**APPENDIX 5: SUB-PROCESSORS**

**1 SUB-PROCESSORS**

1.1 Authorised list of sub-processors are:

| Name | Purpose | Location |
|---|---|---|
| Microsoft Azure | Processing infrastructure | where Service Provider is Deel Software Solutions (Pty) Ltd or Letsdeel Mauritius Inc, Johannesburg - South Africa: South Africa<br><br>where Service Provider is Deel Software Solutions (UK) Ltd, London - United Kingdom: Netherlands |
| Microsoft Azure | Disaster recovery and business continuity processing | European Union |
| Deel Inc, Deel Group | Affiliate | Various Locations |

**Data Processing Addendum – Appendix 6: Jurisdiction Specific Terms**

**APPENDIX 6: JURISDICTION SPECIFIC TERMS**

**1 AUSTRALIA**

1.1 The definition of "Non-EU Data Protection Laws" includes the Australian Privacy Principles and the Australian Privacy Act (1988).

1.2 The definition of "personal data" includes "Personal Information" as defined under Australian data protection law.

1.3 The definition of "Sensitive Data" includes "Sensitive Information" as defined under Australian data protection law.

**2 BOTSWANA**

2.1 The definition of "Non-EU Data Protection Laws" includes the Data Protection Act, No. 32 of 2018.

**3 BRAZIL**

3.1 The definition of "Non-EU Data Protection Laws" includes the Lei Geral de Proteção de Dados (General Personal Data Protection Act).

3.2 The definition of "Security Incident" includes a security incident that may result in any relevant risk or damage to data subjects.

3.3 The definition of "processor" includes "operator" as defined under Brazilian data protection law.

**4 CANADA**

4.1 The definition of "Non-EU Data Protection Laws" includes the Federal Personal Information Protection and Electronic Documents Act.

**5 EUROPEAN ECONOMIC AREA (EEA)**

5.1 The definition of "EU/UK Data Protection Laws" includes the General Data Protection Regulation (EU 2016/679) ("GDPR").

**6 ISRAEL**

6.1 The definition of "Non-EU Data Protection Laws" includes the Protection of Privacy Law.

6.2 The definition of "Controller" includes "Database Owner" as defined under Israeli data protection law.

6.3 The definition of "processor" includes "Holder" as defined under Israeli data protection law.

**7 JAPAN**

7.1 The definition of "Non-EU Data Protection Laws" includes the Act on the Protection of Personal Information ("APPI").

7.2 The definition of "personal data" includes information about a specific individual applicable under Section 2(1) of the APPI.

**8 KENYA**

8.1 The definition of "Non-EU Data Protection Laws" includes the Data Protection Act, 2019 and its Regulations.

**9 MEXICO**

9.1 The definition of "Non-EU Data Protection Laws" includes the Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations.

**10 NIGERIA**

10.1 The definition of "Non-EU Data Protection Laws" includes the Nigeria Data Protection Act 2023 ("NDPA").

**11 SINGAPORE**

11.1 The definition of "Non-EU Data Protection Laws" includes the Personal Data Protection Act 2012 ("PDPA").

**Data Processing Addendum – Appendix 6: Jurisdiction Specific Terms**

**12 SOUTH AFRICA**

12.1 The definition of “Non-EU Data Protection Laws” includes the Protection of Personal Information Act 2013 (“POPIA”)

12.2 The definition of “Personal Data” includes “Personal Information” as defined under POPIA.

12.3 The definition of “Controller” includes “Responsible Party” as defined under POPIA.

12.4 The definition of “Data Processor” includes “Operator” as defined under POPIA.

12.5 The definition of “Sensitive Data” includes “Sensitive Personal Information” as defined under POPIA.

**13 SWITZERLAND**

13.1 The definition of “Non-EU Data Protection Laws" includes the Swiss Federal Act on Data Protection, as revised (“FADP”).

**14 UNITED KINGDOM (UK)**

14.1 The definition of "EU/UK Data Protection Laws" includes the UK GDPR and Data Protection Act 2018.

14.2 “UK GDPR” has the same meaning as defined in section 3 of the Data Protection Act 2018.

**15 UNITED STATES OF AMERICA**

15.1 The definition “Non-EU Data Protection Laws” includes all state laws relating to the protection and processing of personal data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act (“CCPA”), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act.

15.2 The definition of “data subject” includes “Consumer” as defined under CCPA.

15.3 The definition of “Controller” includes “Business” as defined under CCPA. The definition of “Data Processor” includes “Service Provider” as defined under CCPA.

15.4 The definition of "Personal Data” includes “Personal Information” as defined under the CCPA.

15.5 The terms “Business Purpose” and “Sell”, shall have the same meaning as in the CCPA.

15.6 Service Provider will process the Personal Information only for the business purposes set forth in the Agreement, including the purpose of processing and processing activities set forth in this Data Processing Addendum. Service Provider will not sell or share Personal Information or retain, use, or disclose Personal Information (i) for any purpose, including for a commercial purpose, other than the ones set forth in this Data Processing Addendum, unless Customer has provided its prior written agreement or as otherwise permitted by the CCPA; or (ii) outside of the direct business relationship between Customer and Service Provider;

15.7 Not combine any Personal Information that Service Provider processes under the Addendum with any information that Service Provider holds of any third party except as permitted by Customer or otherwise expressly permitted by Applicable Laws;

**16 CHINA**

16.1 The definition of ““Non-EU Data Protection Laws” includes the Personal Information Protection Law (PIPL).

16.2 The definition of "Personal Data” includes “Personal Information” as defined under the PIPL.

16.3 The definition of “Sensitive Data” includes “Sensitive Personal Information” as defined under the PIPL.

16.4 The definition of “Controller” includes “Personal information Handler” as defined under the PIPL.

**17 HONG KONG**

17.1 The definition of “Non-EU Data Protection Laws” includes Hong Kong's Personal Data (Privacy) Ordinance (Cap. 486) as amended in 2012 ('PDPO').

## APPENDIX 7: RETENTION AND / OR DELETION OF PERSONAL DATA

### 1 PROCESS FOR OBTAINING DATA AT END OF CONTRACT PERIOD

1.1 Upon expiry or termination of the Agreement, Customer will have a period of thirty (30) days from the effective date of expiry or termination to download or export its Personal Data using any secure data retrieval mechanisms made available by the Service Provider, including but not limited to reports, web services, or business intelligence tools.

1.2 Upon expiry of the thirty (30) day period described in clause 1.1 above, Service Provider will disable Customer's account. Thereafter, the Customer will have no further access to any Personal Data stored or previously processed by the Service Provider.

### 2 DELETION OF PERSONAL DATA

2.1 If Customer requests deletion of its Personal Data, Service Provider will, as soon as reasonably practicable after receipt of such request, delete or destroy all copies of Customer's Personal Data in its systems or otherwise in its possession or under its control, unless retention is required by applicable law.

2.2 Following the deletion or destruction of the Personal Data as contemplated in clause 2.1 above, Service Provider will provide Customer with written certification that such deletion or destruction is complete, within one (1) month of completion.

### 3 VALUE ADDED HISTORICAL INFORMATION SERVICE

3.1 If Customer does not request deletion of its Personal Data in writing within the period specified in clause 1.1 above:

3.1.1 The Personal Data will, after the expiry of the thirty (30) day period referenced in clause 1.1, be retained by Service Provider for the limited and lawful purpose of providing chargeable, historical enquiry and reporting services to Customer.

3.1.2 Service Provider will continue to apply appropriate technical and organisational safeguards to such retained Personal Data, equivalent to those deployed during the term of this Agreement.

3.1.3 The Service Provider warrants and undertakes that such retained Personal Data will not be accessed or used for any purpose other than those expressly stated in this Appendix.

3.1.4 Access to retained Personal Data for historical information purposes will be subject to a mandatory payment by Customer of a fee equal to fifty percent (50%) of the last applicable subscription fee paid by Customer, payable in advance and recurring monthly, unless otherwise agreed in writing. Such access will continue until Service Provider receives a written instruction from Customer to delete the Personal Data, upon which clause 2 above shall apply.

### 4 GENERAL

4.1 Nothing in this Appendix will relieve either Party of its data protection law obligations.

4.2 Any certification of deletion provided under this Appendix will constitute conclusive evidence that Service Provider has complied with its personal data deletion obligations in respect of Customer's Personal Data.