Data Processing Addendum (DPA)

Deel Client Controller to Controller DPA – Version November 2020

Between

Deel. Inc,

a Delaware registered company,

having its headquarters at:

650 2nd St, 94107, San Francisco, California, United States

(hereinafter "Deel")

And

Client Name: ……………………………………………………………………

………………………………………………………………

Client Address: ………………………………………………………………

..………………………………………………………………

..………………………………………………………………

(hereinafter "Client")

(individually, the "Party" and collectively, the "Parties")

Table of contents

1. Purpose

1. This Processing Addendum ("DPA") forms a part of the Deel Terms of Service found at https://www.letsdeel.com/terms-of-service, unless Client has entered into a superseding written subscription agreement with Deel, in which case, it forms a part of such written agreement (in either case, the "Agreement").
2. Deel and Client have entered into the Agreement for the provision of services. This Data Processing Addendum (hereinafter "DPA" or "Addendum") and its applicable DPA Annexes apply to the Processing of Personal Data by Parties subject to the Data Protection Laws in order to provide services ("Services") pursuant to the Agreement between Deel and Client.
3. As part of their contractual relations, the Parties shall undertake to comply with the applicable Data Protection Laws on personal data processing.

2. Definitions

"Data Protection Laws" means all data protection laws and regulations applicable to a party's processing of Client's Personal Data under the Agreement, including, where applicable, EU Data Protection Laws and Non-EU Data Protection Laws.

"EU Data Protection Laws" means all data protection laws and regulations applicable to Europe, including (i) Regulation (EU) 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) ("GDPR"); (ii) applicable national implementations of (i); and (ii) in respect of the United Kingdom ("UK") any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the UK leaving the European Union, and (iii) data protection laws and regulations of Switzerland.

"Europe" means, for the purposes of this DPA, the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom.

"Non-EU Data Protection Laws" means the California Consumer Privacy Act ("CCPA"); the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"); and the Brazilian General Data Protection Law ("LGPD"), Federal Law no. 13,709/2018, and its implementing regulations.

Capitalized terms used in this DPA shall have the same meaning given to them under Data Protection Laws or if not defined thereunder, the GDPR, unless a different meaning is specified herein. In regards to the CCPA, terms used in the applicable provisions of the DPA where the CCPA is the applicable law shall be replaced as follows: "Personal Data" shall mean "Personal Information"; "Controller" shall mean "Business"; "Processor" shall mean "Service Provider"; and "Data Subject" shall mean "Consumer".

3. Contractual documents

This Addendum and its Annexes constitute the entire Data Processing Agreement between the Parties. It replaces all previous agreements relating to its object. Any prior agreements between the Parties relating to personal data, are not binding on the Parties.

The contractual documents must be interpreted as forming a coherent and inseparable whole, with each of them complementing and being explicit in both technical and legal terms. In the case of a divergence between these documents, the decreasing order of priority is defined as follows:
- This document,
- Annex 1 Personal Data
- Annex 2 Technical and organisational measures
- Annex 3 Contact details of the parties

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 Annexes without a document signed by both Parties.

4. Duration of the assignment/notice of termination

1. The duration of the assignment, (term of the contract) depends on the duration of the service agreement under the Agreement.
2. The termination of this Amendment therefore depends on the provisions concerning the duration and the termination of the Agreement. Notice to terminate the Agreement shall also have the effect of terminating this Addendum.
3. Furthermore, the premature termination of this Addendum without notice shall be permissible in the event of a serious breach of statutory or contractual data protection provisions, insofar as the contracting Party in question cannot reasonably be expected to continue this Addendum.
4. The parties acknowledge that the termination of the Addendum at any time and for any reason, does not exempt them from their obligations relating to the collection, processing and use of personal data on behalf of another.

5. Processing of Personal Data – arrangement between independent controllers

1. The parties agree that Deel and Client are independent Controllers with respect to the processing of such Personal Data under this DPA as described in **Annex 1**.
2. The purpose(s) and nature of operations carried out on the data is the one described in the Agreement.
3. To perform the Services covered herein, the Client shall provide Deel with all the necessary information
4. Each party will comply with the obligations applicable to it under the Data Protection Laws with respect to the processing of Personal Data covered under this DPA.

6. Processors

1. Client acknowledges and agrees that Deel may engage third-party Processors in connection with the provision of the Services. Deel acknowledges and agrees that Client may engage third-party Processors in connection with the receipt of the Services. Both parties will have a written

agreement with each Processor and agree that any agreement with a Processor will include substantially the same data protection obligations as set out in this DPA.

2. Both parties shall be liable for the acts and omissions of its Processors to the same extent such party would be liable under the terms of this DPA, except as otherwise set forth in the Agreement.

7. Technical and organisational measures

1. Deel shall take suitable technical and organisational measures appropriate to the risk to ensure for protection of the security, confidentiality and integrity of Personal Data it Processes under this DPA. Deel guarantees that it has carried out the technical and organisational measures specified in **Annex 2** to this agreement.

2. The technical and organisational measures are subject to the current state of technology and technical progress. In this regard, Deel is permitted to implement adequate alternative measures. These measures may not fall below the level of security of the stipulated measures.

8. Cross-border data transfers

1. If the Services involve the storage and/or Processing of Personal Data which transfers Personal Data out of the Europe to a jurisdiction that does not have adequate data protection laws, and the Data Protection Laws apply to the transfers of such data ("Transferred Personal Data"), both parties agree that the Standard Contractual Clauses for transfers reflecting the roles of the parties as described DPA in the form approved by the European Commission and available at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en (as amended or updated from time to time) ("Standard Contractual Clauses") shall be incorporated by reference and form an integral part of this DPA. Purely for the purposes of the descriptions in the Standard Contractual Clauses the parties agree that the roles of "data importer" and "data exporter" under the Standard Contractual Clauses are as described in this DPA. Further, **Annex 1 Annex 2** of the DPA will take the place of Appendixes 1 and 2 of the Standard Contractual Clauses respectively.

2. If the Standard Contractual Clauses are deemed invalid by a governmental entity with jurisdiction over Transferred Personal Data (e.g., the EU Court of Justice) 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.

3. To the extent Client is the recipient of Personal Data from Deel pursuant to the Agreement, Client will provide at least the same level of protection for the information as is available under the Standard Contractual Clauses.

9. Final provisions

4. 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.

5. 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.

6. 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.

7. This Addendum and all transactions carried out in performing this Addendum shall be governed by local law and, insofar as applicable, the General Data Protection Regulation.

8. The Parties agree to submit to the exclusive jurisdiction of the court of local jurisdiction any claim or dispute arising from this Addendum.

Signatories

On behalf of Client:

Customer Full Legal Name: ……………………………………………………………

Signatory Name ……………………………………………………………

Position: ……………………………………………………………

Date, Signature: ……………………………………………………………

On behalf of Deel:

Deel Full Legal Name: **Deel. Inc**

Signatory Name **Alex Bouaziz**

Position: **CEO**

Signature:

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

- ✓ Client's representatives and Deel Platform users of the Client such as employees, contractors and collaborators of the Client.

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

- ✓ *Contact information*: name, addresses, e-mail addresses, phone numbers and other ways in which Deel can contact the data subject
- ✓ *Identity verification data:* To verify an individual's identity, we may collect an individual's date of birth, taxpayer or government identification number, or a copy of a government-issued identification. In this identification verification process, we also may collect a selfie in order to be able to verify someone's identity by determining whether a selfie taken matches the photo in the government-issued identification. For this, the facial recognition technology collects information from the photos that may include biometric data. We also may collect information from third parties, such as credit bureaus, identity verification services, and other screening services to verify that the individual is eligible to use our Services.
- ✓ *Communications:* any communication Client has with Deel, like emails and phone calls
- ✓ *Information regarding the usage of the Deel Platform,* like payment transactions and technical connection data (IP address, location, logs, etc.)

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

- ✓ *Biometric data*

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

- ✓ storage and other processing necessary to provide, maintain and update the Services provided to the Client
- ✓ to provide technical support to the Client
- ✓ disclosures in accordance with the Agreement, as compelled by law

Annex 2: Technical and organisational measures

Deel has implemented comprehensive organisational and technological measures to ensure the safety of the personal data as well as undisturbed operation in an optimal manner.

The following technical and organisational measures have been taken:

a) Admission control:
Measures to prevent unauthorised persons from gaining access to the data processing equipment used to process personal data.

Imple-mented	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 Deel staff

b) Access control:
Measures and procedures to prevent unauthorised persons from using the data processing equipment.

Imple-mented	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 GDPR
Y	Role based authorization
Y	Controlled destruction of data carriers
Y	Regular security audit

c) Access monitoring:
Measures to ensure that those authorised for data processing can only access the personal data subject to their access authorisation.

Imple-mented	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

d) Transfer control:

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

Imple-mented	Measure
Y	Guidelines for the exchange of information of all kinds
Y	Encryption during data transmission (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

e) Input control:

Measures to ensure authenticated entry of personal data.

Imple-mented	Measure
Y	Access control
Y	Data security policy
Y	Process, program and workflow organization

f) Order control:

Measures to ensure that personal data processed on behalf of the Controller can only be processed in accordance with the Controller's instructions.

Imple-mented	Measure
Y	Contract in writing with determination of the instructions
Y	Formalized order placement
Y	Careful selection of the subcontractor
Y	Monitoring the proper execution of the contract
Y	Separation of duty

g) Availability control:

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

Imple-mented	Measure
Y	Controlled process to ensure business operations (BCM)/IT-SCM
Y	contingency plans
Y	Regular back-ups according to backup plan
Y	Protection of systems against database failure, service level agreements with IT service providers
	Mirroring of data

Imple-mented	Measure
Y	Antivirus/Firewall
Y	Redundant hardware

h) <u>Separation control:</u>
Measures to ensure that data collected for different purposes can be processed separately.

Imple-mented	Measure
Y	Client separation
Y	Functional separations

i) <u>Procedures for periodic review and evaluation</u>
Procedures for regular review, evaluation and evaluation of the effectiveness of technical and organisational measures

Imple-mented	Measure
Y	Data Protection Management
Y	Incident response management

Annex 3: Contact details of the parties

Parties entitled to issue instructions and recipients of instructions

Deel

Name	Address	Email
Bouaziz & Partners	45 Quai de la Seine, 75019, Paris	dpo@letsdeel.com

Client

Name	Address / Telephone	Email
……………………………………	……………………………………	……………………………………

Deel's Data Protection Officer

Name	Address / Telephone	Email
Bouaziz & Partners	45 Quai de la Seine, 75019, Paris	dpo@letsdeel.com

Client's Data Protection Officer (if applicable)

Name	Address / Telephone	Email
……………………………………	……………………………………	……………………………………