**EU Data Transfer Agreement**

**DATA PRIVACY AND SECURITY**

This Data Transfer Agreement("DTA") covers and applies to the transfer of personal information from Uber B.V. ("UBER") to the "Card Issuer" in response to any and all recurring request(s) for data from the Card Issuer to identify the fraudulent use of a credit card of one of its card holders for payments of services purchased via the Uber app ("the Purpose").

Unless otherwise stated in this DTA, undefined, capitalized terms in this DTA shall have the meanings set forth in the Agreement. Nothing in this DTA shall limit or reduce any of Card Issuer's obligations under the Agreement, including without limitation with regard to Confidential Information.

1. **Definition**

"Personal Data" means any information obtained in connection with this DTA (i) relating to an identified or identifiable natural person; (ii) that can reasonably be used to identify or authenticate an individual, including but not limited to name, contact information, precise location information, persistent identifiers, government-issued identification numbers, passwords, or PINs, financial account numbers and other personal identifiers; and (iii) any information that may otherwise be considered "personal data" or "personal information" under the applicable law.

2. **Data Restrictions**

2.1. Card Issuer agrees to collect only such Personal Data as is necessary to provide the Purpose, and for no other purpose, unless expressly authorized in writing by UBER.

2.2. Card Issuer shall maintain the accuracy and integrity of any Personal Data in its possession, custody or control.

2.3. Card Issuer shall not collect, use, disclose, store, retain or otherwise process any Personal Data in connection with the Purpose other than the Personal Data provided to it by or on behalf of UBER or its Affiliates.

2.4. Except as authorised by UBER or as necessary for the Purposes , Card Issuer shall not take steps to de-identify, anonymize or aggregate Personal Data.

2.5. For the avoidance of doubt, Card Issuer shall not, and shall not permit any third party (including without limitation its Affiliates) to, rent or sell Personal Data, for any purpose, including marketing. Card Issuer shall not use Personal Data in any way that harms UBER or that benefits a competitor of UBER.

3. **Legal Security Measures**

3.1. **Compliance with Applicable Law**. In addition to the representations and warranties provided in the Agreement, Card Issuer hereby represents and warrants that:

a. Card Issuer is in compliance, and shall remain in compliance during the Term of the Agreement, with all applicable local, city, state, federal, national, and international laws, rules and regulations relating to data protection, privacy, encryption, identity theft, data breach, consumer protection, and data security, and any applicable industry standards relating to privacy and data security (collectively, "**Data Privacy Laws**"); and

b. Card Issuer will assist UBER in complying with all applicable Data Privacy Laws, including in circumstances where such Data Privacy Laws are directly applicable to UBER but not directly applicable to Card Issuer to the extent such compliance relates to the Purpose.

3.2. **Compliance with Agreement**. Without limiting any of Card Issuer's responsibilities for Personnel under the DTA, Card Issuer shall ensure that all Personnel who have access to any Personal Data are aware of and comply with the applicable terms of this DTA.

3.3. **Third Parties**.

a. Consultant agrees that it shall not disclose Personal Data to any third party, including subcontractors and affiliates, except as permitted under this DTA.

b. Card Issuer shall not use the services of any third party for the processing of Personal Data without UBER's prior written approval in each case. If UBER approves such processing by a third party ("**Approved Third Party**"), Card Issuer shall ensure that each such Approved Third Party is aware of and bound by this DTA and the Standard Contractual Clauses, if applicable, prior to receiving access to any Personal Data.

c. Card Issuer shall be liable for any noncompliance with or breach of the Agreement (including without limitation this DTA) by an Approved Third Party. As between UBER and Card Issuer, Card Issuer is solely responsible for all expenses, fees and costs related to engaging an Approved Third Party. If Card Issuer becomes aware of any violation of the terms of this DTA by an Approved Third Party, Card Issuer shall notify UBER promptly and shall assist UBER with any investigation thereof. In the event UBER determines that an Approved Third Party has violated or breached this DTA, UBER may, at its option, require Card Issuer to (a) promptly cease allowing such Approved Third Party to have access to or use Personal Data; and (b) cause the Approved Third Party to promptly destroy or return (at UBER's election) any Personal Data in its possession, custody or control. If Card Issuer fails to do so, in addition to any rights and remedies as may be available to UBER under the law or equity, UBER shall have the right to immediately terminate the DTA.

4. **Organizational Security Measures**

4.1. **Point of Contact**. Card Issuer shall appoint a representative to act as a single point of contact for UBER with respect to this DTA ("**Privacy Representative**"). The Privacy Representative shall be responsible for ensuring Card Issuer's compliance with this DTA.

4.2. **Security Program**. Card Issuer represents, warrants, and covenants that Card Issuer has developed and implemented, and will consistently update and maintain as needed: (i) a written and comprehensive information security program in compliance with applicable Data Privacy Laws; and (ii) reasonable policies and procedures designed to detect, prevent, and mitigate the risk of data security

breaches or identify theft ("**Security Program**"). Specifically, the Security Program shall include, at a minimum:

a. a data loss prevention program, with appropriate policies and/or technological controls designed to prevent loss of Confidential Information and Personal Data through personal email, peripheral devices (including USB and CD/DVD media), and other means; and

b. a disaster recovery/business continuity plan that addresses ongoing access, maintenance and storage of Confidential Information and Personal Data as well as security needs for back-up sites and alternate communication networks.

4.3. **Training**. Card Issuer shall provide appropriate training to its personnel and any Approved Third Party to ensure they comply with the Agreement, including without limitation this DTA, with regard to Confidential Information and Personal Data. Card Issuer shall provide such training to Personnel and any Approved Third Party before they are allowed access to Confidential Information or Personal Data and no less than annually thereafter. Such training shall be consistent with industry best practices. Upon reasonable notice from UBER, Card Issuer will provide UBER with summaries or copies of Card Issuer's relevant training program.

4.4. **Access**. Card Issuer shall limit disclosure of and access to Personal Data to only those personnel who have a business need to access Personal Data in order to provide the [SERVICES][SOFTWARE]to Uber. Card Issuer shall establish, maintain, and enforce the security principles of "segregation of duties" and "least privileged access" with respect to all Personal Data. Card Issuer shall reasonably update all access rights based on personnel or computer system changes, and shall periodically review all access rights at an appropriate frequency to ensure current access rights to Personal Data are appropriate and no greater than are required for an individual to perform his or her functions necessary for the Purpose. Card Issuer shall verify all access rights through effective authentication methods.

4.5. **Background Investigations of Personnel**. Card Issuer agrees that any Personnel or of any subcontractor who have access to r Personal Data shall have passed a background check. Each background check shall include the following minimum review of all Personnel: identity verification (utilizing Social Security numbers or other state/national ID number) and a criminal history check. Background checks must be performed by a member of the National Association of Professional Background Screeners or a competent industry-recognized Consultant with the same level of professionalism within Consultant's jurisdiction.

5. **Technical and Physical Security Measures.**

5.1. **Encryption**. Card Issuer shall encrypt all Personal Data in its possession, custody or control while in transit or at rest. For the avoidance of doubt, "encryption" shall be deployed using PGP or other industry best practice for key-based encryption protocol. Card Issuer shall have in place appropriate technology to receive, store, and transmit the Personal Data in an encrypted format, and Card Issuer will work with UBER to test Card Issuer's ability to deliver the data in an encrypted form to UBER.

5.2. **Security Patches**. Card Issuer shall deploy all applicable and necessary system security

patches to all software and systems that process, store, or otherwise have access to the Personal Data, including operating system, application software, database software, web server software within industry best practices and in accordance with its information security policies.

5.3. **Virus/Malware Scanning**. Card Issuer shall use up-to-date, industry standard, commercial virus/malware scanning software that identifies malicious code on all of Card Issuer's systems that collect, use, disclose, store, retain or otherwise process Personal Data. For purposes of this agreement, "virus/malware" refers to any programming routines intended to damage, surreptitiously intercept or expropriate any system data or personal information.

5.4. **IT Systems**. Card Issuer shall protect its own information technology systems against malicious code and ensure that its connection to the Internet (including without limitation any platform or network used for the Purpose is secure. In addition, Card Issuer shall acquire and implement new information technology systems as they become available and are proven stable in accordance with industry standards, including without limitation systems designed to monitor hardware and software.

5.5. **Access Control and Limiting Remote Access**. Card Issuer shall secure its computer networks using multiple layers of access controls to protect against unauthorized access. Except as otherwise set forth in the DTA, Card Issuer shall limit processing and storage of Personal Data to internal applications residing within Card Issuer's internal network, and prevent access to Personal Data via an Internet facing application or system. Card Issuer shall secure access to and from its systems by disabling remote communications at the operating system level if no business need exists and/or by restricting access through management approvals, robust controls, logging, and monitoring access events and subsequent audits. Card Issuer shall identify computer systems and applications that warrant security event monitoring and logging, and reasonably maintain and analyze log files.

5.6. **Data Segregation**. Card Issuer shall not merge or combine Personal Data with any other data set and shall maintain all Personal Data in segregated logical access restricted folders or systems.

5.7. **Labeling**. Card Issuer shall use commercially reasonable efforts to limit the appearance of Personal Data on physical media, including paper documents. In any event, Card Issuer shall control and protect access to such physical media to avoid loss or damage thereof. Card Issuer shall ensure safe and secure storage, transfer, exchange, and disposal of all such physical media. If Personal Data is stored on media off-site for back-up purposes, such media shall not include any visible label identifying or listing UBER's name.

5.8. **Server Location**. Card Issuer shall host all Personal Data on servers that are physically located in the EU, unless otherwise agreed in writing by the parties. Card Issuer acknowledges and agrees that if it is necessary to host Personal Data in any other location(s), Card Issuer must still comply with all applicable Data Privacy Laws, including without limitation those of the country to which and from which Card Issuer may transfer Personal Data.

5.9. **Third-Party Data Centers**. If Card Issuer uses a third-party data center to host the Personal Data, Card Issuer shall ensure that (i) all application and database servers are physically isolated within the data center and secured from unauthorized physical access; (ii) physical and network access is limited to Card Issuer's Personnel or Approved Third Party; and (iii) any use of a shared

environment does not compromise the security, integrity, or confidentiality of Personal Data.

6. **Security Reviews by Uber.**

6.1. **Internal Audits**. Upon UBER's written request, Card Issuer shall provide UBER, at Card Issuer's expense, with the results of the most recent data security compliance reports or any audit performed by or on behalf of Card Issuer that assesses the effectiveness of Card Issuer's information security program, system(s), internal controls, and procedures relating to the Personal Data (e.g., SSAE16, SOC report or other). Such reports shall be of sufficient scope and in sufficient detail as may reasonably be required by UBER to provide reasonable assurance that any material inadequacies would be disclosed by such examination (including without limitation summaries of any control issues and associated corrective action plans and management responses), and, if there are no such inadequacies, the reports shall so state.

6.2. **External Audits**. UBER may, not more than once per year, during normal hours of business and with reasonable advance written notice to Card Issuer, at its own expense, audit, or designate a third party to audit, Card Issuer's facilities, networks, systems, procedures, processing and maintenance of Personal Data, and compliance with its obligations under the DTA.Notwithstanding the foregoing, UBER shall be permitted to exercise such audit right any time an Information Security Incident (as defined below) has occurred or is reasonably believed to have occurred. Card Issuer shall reasonably cooperate with such audit by providing access to knowledgeable personnel, physical premises as applicable, documentation, infrastructure, and any application software that processes Personal Data or otherwise has access to UBER's networks and systems. UBER shall be responsible for its costs and expenses of such audit (or the fees and costs of the third party performing the audit), unless such audit reveals a material breach of this DTA, in which case Card Issuer will reimburse UBER for such costs and expenses. Card Issuer will promptly address and correct all deficiencies identified in any such audit.

6.3. **Vulnerability Testing**. Upon reasonable prior notice to Card Issuer, UBER may periodically (but not more frequently than once per year) perform vulnerability tests on Card Issuer's networks, software and systems to confirm Card Issuer's compliance with this DTA. Card Issuer will promptly address and correct all security vulnerabilities identified in a vulnerability test or report.

6.4. **Source Code Audit**. Upon UBER's request, Card Issuer will provide the then-current source code for any software that has access to or processes Personal Data to an independent third-party auditor selected by UBER. Such third-party auditor may review the software and Card Issuer will be responsible for the costs of this audit. To the extent the third-party auditor identifies any vulnerabilities, Card Issuer will be solely responsible for and will bear all costs related to the removal of such vulnerabilities. Card Issuer will provide UBER with a corrective action plan to address the removal of such vulnerabilities, which will include an estimated timeline for remediating such vulnerabilities.

7. **Retention and Disposal**

7.1. **Data Retention**. Card Issuer shall retain material containing Personal Data only so long as necessary for the Purpose.

8. **Information Security Incident Response.**

8.1. Card Issuer agrees to implement appropriate legal, administrative, technical, physical and organizational measures, including those described in this DTA, to protect Personal Data in accordance with industry standards and practices against unauthorized or unlawful processing, access or disclosure and against unauthorized or accidental loss, destruction, damage, alteration, as well as any breach or attempted breach of Card Issuer's security measures ("**Information Security Incident**"), keeping in mind the nature of the information.

8.2. **Notification**. Card Issuer shall notify Uber at VendorSecurity@uber.com within 24 hours in the event that Card Issuer learns or has reason to believe that an Information Security Incident has occurred or is reasonably likely to occur, including at least: (1) the nature of the breach of security measures; (2) the types of potentially compromised Personal Data; (3) the duration and expected consequences of the Information Security Incident; and (4) any mitigation or remediation measures taken or planned in response to the Information Security Breach.

8.3. **Information Security Incident Response**. In connection with any Information Security Incident, Card Issuer shall immediately and to the extent reasonably possible (a) take all reasonable steps to investigate, remediate, and mitigate the effects of the Information Security Incident, and (b) provide UBER with assurances reasonably satisfactory to UBER that such Information Security Incident will not recur. Further, Card Issuer shall fully cooperate with UBER's investigation into the Information Security Incident and provide all necessary information, access and materials necessary to satisfy UBER's investigation and resolution of the Information Security Incident. All information exchanged in connection with this investigation shall be deemed to be UBER's confidential information. Notwithstanding anything to the contrary in this Agreement, Card Issuer understands and agrees that UBER has the right to disclose confidential information to third parties as necessary to assist in the investigation and resolution of an Information Security Incident.

8.4. **Remedial Measures**. Card Issuer shall be responsible for all costs related to or arising from any Information Security Incident to the extent such Information Security Incident occurs as a result of an act or omission of Card Issuer, its Affiliate or either of its or their respective employees or of any Approved Third Party. Without limiting the foregoing, Card Issuer acknowledges and agrees that an Information Security Incident may require (a) an investigation of the Information Security Incident; (b) the tracking and recovering of Personal Data; (c) providing notifications (whether in UBER's or Card Issuer's name) to (i) all individuals affected by the Information Security Incident and (ii) state, federal, or international law enforcement or regulatory agencies/bodies; and/or (d) providing other remedies to the individuals affected by the Information Security Incident. The provision of such notifications, if any, including the contents thereof, shall be determined by UBER in its sole discretion.

9. **Investigations and Data Subject Requests**

9.1. **Regulatory Investigations and Requests**. Card Issuer shall provide UBER with reasonable assistance and support in the event of an investigation by a data protection regulator or other governmental authority, if and to the extent that such investigation relates to the collection, maintenance, use, processing or transfer of Personal Data by or on behalf of Card Issuer. Should any regulatory body require or request a security audit or review, Card Issuer shall, with UBER's involvement (including UBER's attendance at any related meetings with federal, state or other government officials) cooperate with any such audit or review. Without limiting the foregoing, Card Issuer shall provide,

following reasonable notice, (i) access to Card Issuer's information processing premises and records, and (ii) reasonable assistance and cooperation of relevant individuals for the purpose of complying with such audit or review.

9.2. **Notice of Third-Party Request**. If Card Issuer receives a request from a third party in connection with any government, court, or law enforcement investigation or proceeding that Card Issuer believes would require it to produce or disclose any Personal Data, then Card Issuer shall, promptly and, to the extent legally feasible, prior to producing or disclosing such information, notify UBER in writing of such request, and reasonably cooperate with UBER if UBER wants to limit, challenge, or protect against the requested production or disclosure, to the extent permitted by applicable law or regulation.

9.3. **Data Subject Requests**. Card Issuer shall promptly notify UBER in writing if Card Issuer receives a request from an individual for access to that individual's Personal Data. Card Issuer shall provide UBER with commercially reasonable cooperation and assistance in connection with any such request. Except as required by applicable data protection laws, Card Issuer shall not disclose the individual's Personal Data directly to the individual other than at the written instruction of UBER. If Card Issuer is unable to produce the Personal Data requested as a result of an act or omission of Card Issuer, Card Issuer shall be responsible for all costs associated with or arising from its inability to produce the Personal Data.

10. **Non-Compliance**. Card Issuer will not materially lessen the security of any system used to collect, use, disclose, store, retain or otherwise process Confidential Information and/or Personal Data during the term of the DTA. Card Issuer shall promptly notify UBER in writing if Card Issuer is unable to comply with the obligations of confidentiality, privacy and security stated in this DTA. Without limiting any other rights or remedies available at law, equity or otherwise, UBER may take any one or more of the following actions: (i) suspend the transfer of Personal Data; (ii) require Card Issuer to cease processing Personal Data; (iii) demand the return or destruction of Personal Data; or (iv) immediately terminate this DTA.

11. **Term and Survival**. This DTA and all provisions herein shall survive so long as, and to the extent that, Card Issuer retains any Personal Data.