PROPRIETARY RIGHTS AGREEMENT FOR NON-UBER EMPLOYEES

I have been assigned for a limited period of time by Hansem Global, Inc. a managed services provider or consulting agency, to perform certain services for Uber Technologies, Inc., ("Uber" or the "Company"). This Agreement is intended to formalize in writing certain understandings and procedures which apply to my temporary assignment with the Company (the "Assignment"). I acknowledge that this Agreement does not make me an employee of Uber and that I am and will remain an employee of the Managed Services Provider or consulting agency.

I understand that during the course of the Assignment, I will have access to critical confidential information belonging to the Company, as described more fully below, and that, regardless of any other agreement I may have with the Managed Services Provider or consulting agency or any other person or entity, I understand that I would not be permitted to perform any services for the Company without agreeing to be bound by this Agreement. In consideration of the foregoing and the mutual covenants set forth herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, I acknowledge and agree as follows:

1. Continued Obligation

I understand and agree that the terms and conditions of this Agreement are effective upon the start of the Assignment, and do not expire, even upon termination and/or completion of the Assignment.

2. No Conflict

While providing services to the Company during the Assignment, I will devote my best efforts to the interests of the Company. During the course of the Assignment, I will not engage in any activities determined by the Company to be in conflict with my services for the Company, or detrimental to the best interests of the Company.

3. Non-Disclosure of Confidential Information

I agree and acknowledge that during the Assignment, I may receive and have access to confidential, proprietary and/or trade secret information concerning the Company and/or its affiliates, including but not limited to the following: (a) software products, programs, applications, and processes utilized by the Company; (b) scientific or technical information, inventions, designs, processes, procedures, formulas, improvements, technologies or methods;
(c) concepts, reports, data, know-how, works-in progress, development tools, specifications, computer software, source code, object code, flow charts and/or databases; (d) the name and/or address of customers or vendors of the Company or information concerning the transactions or relations of customers or vendors of the Company with the Company; (e) information concerning products, services, technologies, or procedures employed by the Company but not generally known to its customers or vendors or competitors, or under development by or being tested by the Company but not at the time offered generally to customers or vendors; (f) information relating to the Company's computer software, computer systems, pricing or marketing methods,

sales margins, cost of goods, cost of material, capital structure, operating results, borrowing arrangements or business plans; (g) information identified as confidential, proprietary or trade secrets in any line of business engaged in by the Company; (h) information that, to your knowledge, the Company ordinarily maintains as confidential, proprietary or considers to be a trade secret; (i) business plans, budgets, advertising, marketing plans, personnel matters, hiring plans and decisions, employee termination plans and decisions, employee compensation information; (j) information contained in the Company's written or oral policies and procedures or manuals; (k) information belonging to customers, vendors or other persons or entities which the Company, to your actual knowledge, has agreed to hold in confidence; and/or (l) written, graphic, electronic data and other material containing any of the foregoing (collectively the "Confidential Information"). During the Assignment and after the termination and/or completion of the Assignment, I shall not, without written consent of the Company, publish or use or disclose to anyone other than authorized Company personnel any Confidential Information. I agree to abide by the Company policies and regulations for the protection of its Confidential Information and I understand and agree that the unauthorized disclosure or misuse of such confidential, proprietary or trade secret information could irreparably damage the Company and/or third parties dealing with the Company.

4. No Solicitation

I agree that the Company has invested substantial time, effort and expense in compiling its confidential, trade secret information and in assembling its present staff of personnel. In order to protect the confidentiality of the Company's proprietary trade secret information, I agree that, after the Assignment ends, I shall not do the following:

1. Solicit or attempt to solicit the sale or distribution of products or services similar to those offered by the Company or related products or services that would replace those offered by the Company, for myself or on behalf of any other company, to any client or prospective client of the Company with the use of Confidential Information of the Company. For purposes of this Agreement, the term "prospective client" is defined as any individual or entity who was solicited, directly or indirectly, by me or any employee of the Company with my knowledge or assistance to do business with the Company, within the twelve (12) month period preceding the end of the Assignment.

2. Solicit any employee or independent contractor to apply for employment with another employer or otherwise leave his/her position with or terminate his/her employment with, or services for, the Company, or otherwise induce any such employee or independent contractor under contract with the Company to breach that contract in order to accept employment with another employer or otherwise leave his/her position with or terminate his/her employment with, or services for, the Company for a period of six months following the end of the Assignment; or

3. aid, assist or counsel any other person, firm or corporation to do any of the above.

5. Invention Disclosure

I hereby agree to promptly disclose to the Company any and all inventions that I develop during the term of the Assignment. I will also disclose to the Company all inventions made, conceived, reduced to practice, or developed by me within six months of the end of the Assignment that resulted from the services I provided to the Company during the Assignment. Such disclosures shall be received by the Company in confidence and do not extend the assignment of inventions disclosed beyond that required by law.

6. Assignment of Inventions

I hereby assign and grant to the Company or its designee, my entire right, title and interest in and to all inventions, works of authorship, developments, concepts, discoveries, ideas, trademarks and trade secrets, whether or not patentable or registrable under copyright or similar laws ("Inventions") which I may solely or jointly develop, conceive or reduce to practice, during the period of the Assignment, except as provided below. I agree that all such Inventions are the sole property of the Company. I further agree that all such Inventions, including works of authorship are "works for hire" for purposes of the Company's rights under copyright laws. I agree to keep and maintain adequate and current written records of all Inventions made by me (solely or jointly with others) during the term of the Assignment. The records will be in the form of notes, sketches, drawings, and any other format that may be specified by the Company. The records will be available to and remain the sole property of the Company at all times. I further agree to assist the Company, or its designee, at the Company's expense, in every proper way to secure the Company's rights in the Inventions and any copyrights, patents, trademarks, and trade secret rights or other intellectual property rights in connection with any such Inventions in any and all countries, including the disclosure to the Company of all pertinent information and data with respect thereto, the execution of all applications, specifications, oaths, assignments and all other instruments which the Company shall deem necessary in order to apply for and obtain such rights and in order to assign and convey to the Company, its successors, assigns, and nominees the sole and exclusive rights, title and interest in and to such Inventions, and any copyrights, patents, trademark and other intellectual property rights relating thereto. I further agree that my obligation to execute or cause to be executed, when it is in my power to do so, any such instrument or papers shall continue after the termination of this Agreement. I understand that any inventions, discoveries or ideas that I have created or possessed prior to the Assignment are specified in Appendix A attached to this Agreement and will not be considered to be the property of the Company.

I understand and agree that the obligations outlined in this Section 6 do not apply to any invention, discovery or improvement that was developed entirely on my own time for which no equipment, supplies, facilities or trade secret information of the Company was used and (a) that does not relate directly or indirectly to the business of the Company or to the Company's actual or demonstrably anticipated research or development, or
(b) that does not result from any services performed by me during the Assignment.

7. Return of Company Property

All correspondence, memoranda, notes, records, databases, reports, plans, documents, equipment, digitally stored information or other property received or made by me in connection with the Assignment, shall be the exclusive property of Uber and must not be removed from Company premises, except as required in the course of the Assignment. I agree to return promptly and deliver all copies thereof to the Company on the termination and/or completion of the Assignment or upon request.

8. Injunctive Relief

The Company and I fully understand that a breach of any of the promises or agreements contained herein will result in irreparable and continuing damage to the other party for which there will be no adequate remedy at law. Accordingly, the Company and I further agree that in addition to any and all remedies available at law or equity (including money damages) that may be pursued by either party, both parties shall be entitled to preliminary injunctive relief without the necessity of proving actual damages and that the Company and/or I shall be entitled to seek such equitable relief in any forum, including a court of law. The Company and/or I may pursue any of the remedies described herein concurrently or consecutively in any order as to any such breach or violation, and the pursuit of one of such remedies at any time will not be deemed an election of remedies or waiver of the right to pursue any of the other such remedies.

9. Notices

Any notice required or permitted by this Agreement shall be in writing and shall be delivered as follows with notice deemed given as indicated: (1) by personal delivery when delivered personally; (2) by overnight courier upon written verification of receipt; (3) by telecopy or facsimile transmission upon acknowledgment of receipt of electronic transmission; or (4) by certified or registered mail, return receipt requested, upon verification of receipt. Notices to me shall be sent to the last known address in Consulting Agency's records or such other address as I may specify in writing. Notices to the Company shall be sent to _____, or to such other address as the Company may specify in writing.

10. No Violation of Prior Trade Secret or Non-Competition Agreements

I represent that the performance of all the terms of this Agreement will not conflict with, and will not breach, any other invention assignment agreement, confidentiality agreement, employment agreement or non-competition agreement to which I am or have been a party. To the extent that I have confidential information or materials of any employer or former employer of mine, I acknowledge that the Company has directed me to not disclose such confidential information or materials to the Company or any of its employees, and that the Company prohibits me from using said confidential information or materials in any services that I may perform for the Company. I agree that I will not bring with me to the Company, and will not use or disclose any confidential, proprietary information, or trade secrets acquired by me prior to the

Assignment. I will not disclose to the Company or any of its employees, or induce the Company or any of its employees to use, any confidential or proprietary information or material belonging to any employers or previous employers or others, nor will I bring to the Company or use in connection with my services for the Company copies of any software, computer files, or any other copyrighted or trademarked materials except those owned by or licensed to the Company. I am not a party to any other agreement that will interfere with my full compliance with this Agreement. I further agree not to enter into any agreement, whether written or oral, in conflict with the provisions of this Agreement.

11. Survival

This Agreement (1) shall survive the Assignment with the Company; (2) does not in any way restrict my right or the right of the Company to terminate the Assignment at any time, for any reason or for no reason; (3) inures to the benefits of successors and assigns of the Company; and (4) is binding upon my heirs and legal representatives.

12. Governing Law

This Agreement shall be governed in all respects by the laws of the _____ and by the laws of the State where I perform services for the Company, as such laws are applied to agreements entered into and to be performed within that State.

13. Severability

Should any provisions of this Agreement be held by a court of law to be illegal, invalid or unenforceable, the legality, validity and enforceability of the remaining provisions of this Agreement shall not be affected or impaired thereby.

14. Waiver

The waiver by the Company of a breach of any provision of this Agreement by me shall not operate or be construed as a waiver of any other or subsequent breach by me.

15. Modification

This Agreement may be amended only by an agreement in writing signed by the parties hereto.

16. Interpretation

This Agreement shall be interpreted in accordance with the plain meaning of its terms and not strictly for or against either party.

17. Voluntary Agreement

I acknowledge and agree that I have reviewed all aspects of this Agreement, have carefully read and fully understand all the provisions of this Agreement, and am voluntarily

entering into this Agreement. I represent and agree that I have had the opportunity to review any and all aspects of this Agreement with the legal, tax or other advisor(s) of my choosing before executing this Agreement.

18. Entire Agreement

This Agreement represents my entire understanding with the Company with respect to the subject matter of this Agreement and supersedes all previous understandings, written or oral. This Agreement may be amended or modified only with the written consent of both me and the Company. No oral waiver, amendment or modification shall be effective under any circumstances whatsoever.

I certify and acknowledge that I have carefully read all of the provisions of this Agreement and that I understand and will fully and faithfully comply with such provisions.

Signature: 

Name: Bryan L. Tagaan

Date: November 19, 2024

APPENDIX A

PRIOR INVENTIONS

1.

2.

3.

_____ Additional sheets attached

Section 2870 of California Labor Code: Application of provision providing that employee shall assign or offer to assign rights in invention to employer.

a. Any provision and employment agreement which provides that an employee shall assign, or offer to assign, any of his or her rights in an invention to his or her employer shall not apply to an invention that the employee developed entirely on his or her own time without using the employer's equipment, supplies, facilities or trade secret information except for those inventions that either:

1. Relate at the time of conception or reduction to practice of the invention to the employer's business, or actual or demonstrably anticipated research or development of the employer; or
2. Result from any work performed by the employee for the employer.

b. To the extent a provision in an employment agreement purports to require an employee to assign an invention otherwise excluded from being required to be assigned under subdivision (a), the provision is against the public policy of this state and is unenforceable.

EXT Work Principles

December 2, 2022

Table of Contents


Summary


Ethical Business Practices & Political Lobbying


Financial Integrity, Records, and Accounting


Conflicts of Interest


Data Privacy and Information Security & Confidential Information


Antitrust and Competition Laws


Respectful Workplace


Reporting Concerns

Uber

EXTs at Uber refers to independent contractors, temporary workers, vendor workers, independent consultants, dispatch workers, staffing agency workers, secondees, or any person that has EXT login credentials. They are employees of the Supplier company of Uber. For the avoidance of doubt, there is no employment relationship (express or implied) between EXTs and Uber. The Supplier company to Uber is expected to comply with Uber's Supplier Code of Conduct which can be found here: https://t.uber.com/SupplierCOCexternal. The Principles below are where Uber outlines its expectations of conduct for the Supplier's employees while on assignment at Uber.

EXTs must adhere to all applicable laws; legal regulations, directives, and guidelines; and all obligations in any contract their supplier has with Uber. As a condition of doing business with Uber and partnering in our mission, we expect EXTs to share in our commitment to **doing the right thing … period.**

Ethical Business Practices

Uber operates its business fairly and ethically and sets a high standard of business integrity. Uber expects the same from EXTs. Uber does not buy market access, business, or policy outcomes.

Uber strictly prohibits the receipt, offer, or payment of bribes, kickbacks, facilitation payments, or the exchange of anything of value (directly or indirectly) intended to advance business interests or provide undue or improper advantages. The exchange of business courtesies, especially with employees of government agencies, is strictly controlled at Uber, so EXTs should consult with their Uber employee contact who will work with Uber's Ethics & Compliance team for advice. Gifts of cash or cash equivalents are never allowed.

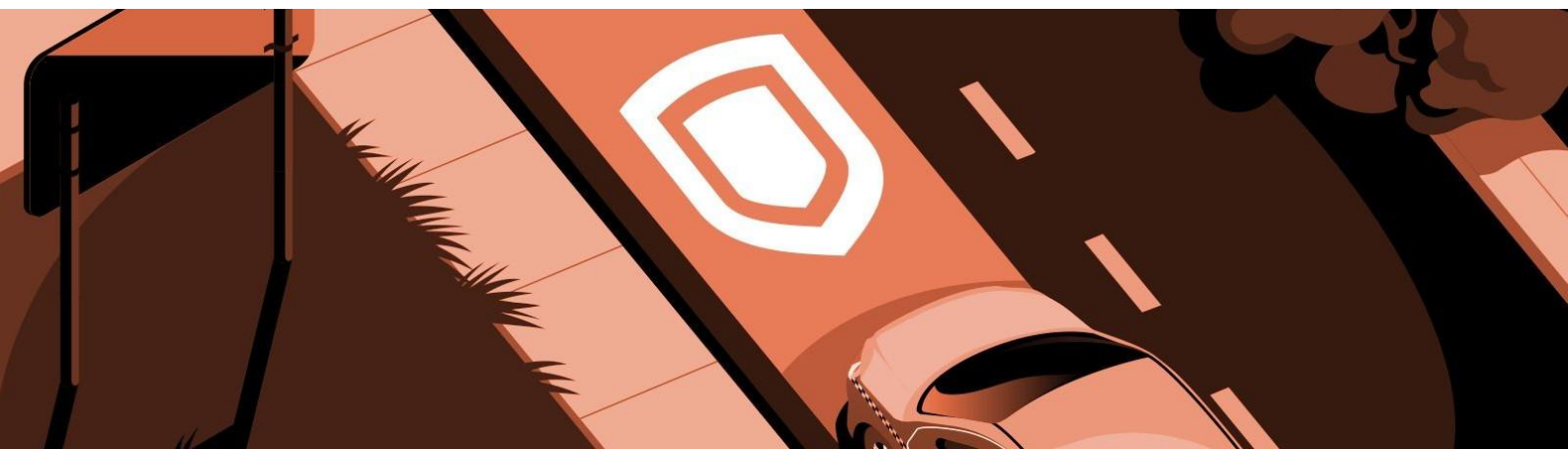
Political Lobbying

Any EXT interacting with a public official must understand and comply with all applicable laws applicable to lobbying. Additionally, Uber has Interaction with Public Officials policies in each jurisdiction which EXTs engaging with public officials must follow.

"Lobbying" generally means any activity that attempts to influence laws, regulations, policies, and rules, and in some countries, it can also mean business development and/or procurement activities.

Financial Integrity, Records, and Accounting

Uber relies on our books and records to report our financial results, make required legal filings, and make business decisions. EXTs must do their part to keep and maintain accurate books and records of all business dealings with and on behalf of Uber in accordance with applicable standard accounting practices.



Fraud

Uber expects EXTs to act honestly and with integrity. Seeking to gain an advantage of any kind by acting fraudulently, stealing, deceiving people or making false claims, or allowing anyone else to do so is prohibited.

Insider Trading

EXTs may have access to material, non-public information about Uber or other companies. Information is **material** if a reasonable investor would consider it important in deciding whether to buy, sell, or hold a company's securities. EXTs may not buy or sell Uber securities while in possession of material, non-public information or provide that information to others who trade on it.

Conflicts of Interest

EXTs must avoid all conflicts of interest (i.e. where the - personal or professional - interests of the EXT interfere with the assignment at Uber) or even the appearance of conflicts of interest. EXTs are expected to promptly disclose to their Uber operational employee contact actual or potential conflicts of interest that could impact Uber. However, working for another company while working for Uber is not by itself a conflict of interest.

Some examples of situations that could create conflicts of interest include:

- Hiring or making an offer of employment to an Uber employee or their family member
- Uber engaging EXT agencies that are owned or controlled, directly or indirectly, by an Uber employee or their family member
- Providing any form of compensation, fees or commissions to Uber employees
- Pursuing or competing for business opportunities that are derived from an EXT's work with Uber
- Obtaining an unfair advantage by acting on information learned through their relationship with Uber
- Any other activity that might adversely affect Uber, our business, or our reputation

Data Privacy and Information Security

EXTs who collect, receive, store or otherwise process personal data in connection with the products or services they provide to Uber must appropriately handle and protect such data (to Uber's satisfaction at all times, before, during and after the relationship with Uber), and comply with all laws, regulations and agreements with Uber applicable to the processing of such data. At no time should an EXT process or send Uber data outside of the Uber corporate network, unless agreed with an Uber Employee who has consulted with our Privacy and Cybersecurity Legal Team.

Confidential Information

EXTs are expected to safeguard all Uber confidential information, electronic data, intellectual property, know-how, and technologies.

EXTs must transfer any such confidential information, electronic data, intellectual property, know-how, or technologies in a way that secures and protects the intellectual property rights of Uber and its business partners.

EXTs may receive Uber's confidential information only as authorized by a confidentiality or non-disclosure agreement and must comply with their obligations to not disclose the confidential information. Also, EXTs must never use any illegal or unethical means to collect or use information about other companies such as competitors to Uber. The EXT should consult with their Uber operational employee contact who will seek guidance from Uber's Ethics & Compliance team for competitive intelligence projects.

Nothing in this document prevents an EXT from disclosing information to a government agency or law enforcement authority.

Antitrust and Competition Laws

Uber is committed to competing fairly for the benefit of consumers and following antitrust and competition laws in the United States and internationally. EXTs working on assignment for Uber must comply with all applicable laws, regulations and standards of fair business, advertising, and competition.

Trade Compliance Laws and Regulations

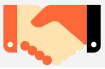
EXTs are responsible for complying fully with all US and global trade laws and regulations, including embargoes and sanctions, and import and export laws that apply to technology, software, intellectual property, and technical information as well as materials and goods.

Anti-Boycott Compliance Laws and Regulations

EXTs are prohibited from participating or supporting any international boycott that is not sanctioned by the United States government.

Anti-Money Laundering Compliance

Money laundering in any form is prohibited. Money laundering includes disguising or concealing the nature, location, source, ownership, or control of unlawfully obtained money, or transforming such money into legitimate funds.



Respectful Workplace

Uber is committed to fostering a respectful workplace - an environment where ALL people are welcome, supported and treated with dignity. EXTs will support Uber's commitment to facilitate a respectful workplace by adhering to the following principles:

- ### Anti-Harassment and Anti-Discrimination

  Uber is committed to the principles of equal opportunity, inclusion and respect. Uber does not tolerate discrimination on the basis of race, color, religion, sex, pregnancy (including childbirth), lactation or related medical conditions, age, national origin or ancestry, physical or mental disability, marital status, medical condition, sexual orientation, gender identity and gender expression, military service status, genetic information or any other status protected by law; nor does Uber tolerate harassment in any form against anyone.

  EXTs must conduct themselves to support a workplace that is free of harassment and abuse, including sexual harassment, corporal punishment, inhumane treatment, or any harassing behavior (verbal, visual, or physical threats or demands) that creates an intimidating, offensive, abusive, or hostile work environment.

  EXTs are expected to support diversity and equal opportunity and shall not engage in unlawful discrimination of any kind.

- ### Labor and Human Rights

  Uber is committed to compliance with human rights laws. We do not use or condone the use of child or involuntary labor or human trafficking. EXTs are prohibited from participating in human trafficking or exploitation, or procuring or supplying goods tainted by human trafficking; using any form of involuntary, slave, forced, bonded, indentured or child labor, regardless of local business customs, or purchasing products or services from companies using involuntary, slave, forced, bonded or indentured labor.

Reporting Concerns

EXTs should promptly report to Uber all violations or suspected violations of these Principles as well as any potential misconduct of an Uber employee. If allowable in the country where the report is lodged, the report can be made anonymously. EXTs can contact their Uber business representative or the Uber Integrity Helpline (https://t.uber.com/Helpline) to report known or suspected misconduct or raise an ethical concern.

Uber takes compliance with these Principles seriously and reserves the right to assess and monitor EXT compliance with them. EXTs are required to complete training relevant to these Principles - either provided by their employer or by Uber - before commencing an assignment at Uber. Violations by EXTs of these Principles will result in a review of the business relationship with the Supplier of the EXT, up to and including termination of the relationship according to Uber's contractual rights and applicable law.

Nothing in these Principles implies an employment relationship between the EXT and Uber, the existence of any subordination from the EXT to Uber, or any change or modification to an employment relationship between a Supplier and an EXT.

Acknowledged by:

Signature

Bryan L. Tagaan
Printed Name

November 19, 2024
Date

Data Access Policy

Policy Owner: Legal - Privacy & Cybersecurity and Security

Confidential

1. Purpose

Uber's Privacy Principles[1] provide that "We safeguard personal data," which requires that we implement "reasonable and appropriate safeguards to prevent loss, and unauthorized use or disclosure, of personal data." Adhering to this principle, as well as privacy laws applicable to Uber, requires that Uber limit internal access to personal data to only those who require it to perform their job responsibilities, and prevent access to such data by anyone else or for any other purpose.

This Policy defines the circumstances when employees may, and may not, Access User Data. The Frequently Asked Questions (FAQs) attached to this Policy provide additional guidance.

2. Scope

All full- and part-time employees are required to read and comply with this Policy. Violations of this Policy may result in disciplinary action up to and including termination.

Uber logs, audits, and monitors employees' access to User Data to ensure compliance with this Policy. Violations of this Policy will be thoroughly investigated, and may result in disciplinary action up to and including termination.

Please email privacylegal@uber.com if you have questions or are unclear regarding the requirements of this Policy.

3. Definitions

For purposes of this Policy:

"Access**"** means searching for, looking up, or using User Data within Uber's network. "Access" does not include viewing or updating one's own data through an Uber app, website or service. Employees are **not** limited under this Policy from viewing or updating their own User Data through Uber apps, websites or services that are available to non-employee Users (*e.g.*, the Uber rider app or www.uber.com).

"User Data" means any information collected by or on behalf of Uber that can be used to identify an actual or potential Uber user (including riders, drivers, delivery recipients, delivery partners or other users of an Uber app, website or service). This includes, but is not limited to, names, addresses, phone numbers, email addresses, passwords, government identification numbers including drivers' licenses and Social Security numbers, photos, background check documents,

[1] *See* Section 4.1 of the above linked Uber Internal Privacy Policy.

application documents, financial information, trip or order history, usage information, user communications, device data, IP addresses, or location information.

4. Requirements

1. You **may not** Access User Data, including your own, unless it is necessary to perform your job responsibilities.

2. You **may not** Access User Data:
    a. of a person you know personally (such as a friend or family member), even if the Access is necessary for your job responsibilities or they have consented to the access.
    b. out of curiosity, to resolve your own customer support issues, or for any other personal reason.

3. Notwithstanding the foregoing, you **may** Access:
    a. your own User Data if necessary to perform your job responsibilities AND alternatives to such Access (such as use of a test account) are not available or feasible; AND
    b. the User Data of a co-worker solely for purposes of de-bugging, if de-bugging is within the scope of your job responsibilities, and your co-worker has consented to the Access.

5. Exceptions or Changes to this Policy

You **may not** Access User Data in violation of the above Policy Rules, unless such Access is necessary to address or resolve a business emergency, such as outages. In such cases, you must notify and explain the justification for the Access to your manager in writing prior to Accessing the User Data.

6. Roles & Responsibilities

This Policy is owned by Legal - Privacy.

This Policy will be reviewed on an annual basis and updated if needed.

7. Review & Revision History

Version	Date	Approved By	Summary of Changes
Version 1.0	04/09/15	Katherine Tassi	N/A
Version 2.0	01/07/17	Derek Care	Streamlined language, clarified

			requirements and updated FAQs
Version 3.0	01/02/19	Ruby Zefo	Streamlined language, clarified requirements and updated FAQs
Version 3.1	06/20/19	Dayo Simms	Added translations links, replaced “data policy” alias with “privacy legal” alias.
Version 3.2	08/26/19	Ruby Zefo	Added exception to section 4 Requirements and clarified access restrictions when de-bugging.
Version 3.3	09/09/2020	Derek Care	Included privacy principle, updated links, and reworded ‘Privacy Legal’ to ‘Privacy & Cybersecurity Legal.
Version 3.4	10/5/2021	Marilyne Fortin	Updated links and made grammatical changes.
Version 3.5	06/02/2022	Derek Care	Reviewed, no changes
Version 3.6	12/27/2022	Derek Care	Specified applicability of Policy to EXTs.
Version 3.7	12/15/2023	Derek Care	Minor grammatical changes

Policy FAQs

1. May I access the account of a friend or family member to help them with a support issue if it is within my role and responsibilities to provide driver or rider customer support?

No. You may not access the accounts of friends or family members. *See* Policy Rule 2(a) (“[Y]ou may not Access User Data … of people you know personally (such as friends, family members, or co-workers), including to resolve their customer support issues.”). This is true even if your responsibilities include addressing customer support issues.

Friends or family members must submit their questions or queries via help.uber.com or the Help menu in the apps to create support tickets and resolve their issues

Employees can escalate unresolved customer support tickets for their friends, family members, acquaintances, or riders and drivers, by contacting teamsupport@uber.com. This support alias is handled by a dedicated group of Customer Support Representatives who can provide quick resolution to user customer support issues.

2. I left a personal item in a driver's car after a trip. May I access my account in Tools to find the driver and then access my driver's account to obtain their contact information?

No. You are prohibited from accessing User Data for personal reasons, including to resolve your own customer support issues. *See* Policy Rule 2(b) ("You **may not** access User Data … to resolve your own customer support issues, or for any other personal reason ").

Employees should instead, direct all personal support issues to help.uber.com for assistance. Employees can also escalate unresolved customer support tickets by contacting teamsupport@uber.com.

3. I need to conduct testing with a user account as part of my role and responsibilities. What should I do?

You should always use test accounts to conduct testing. You can find information on how to create a test account on Team.dot. You can reach the Test Accounts Team on uChat at 'Test Accounts Support.' If using a test account is not feasible, you may use your own account.

4. I am an engineer and my friend reported having problems with the rider app. Can I access his account to determine if there is an outage or bug?

Accessing your friend's account is prohibited, except in the event of a business emergency such as an outage. *See* Policy Rule 2(a) ("You **may not** access User Data of people you know personally, such as friends, families and co-workers."). Instead, if there is no business emergency, you should pass the information to a colleague who does not personally know your friend. The colleague can access your friend's account to determine if there is an outage or bug.

If you believe your friend's issue is indicative of a business emergency such as an outage, you may access their account solely as necessary to address or resolve the issue. You must also notify and explain the justification for the Access to your manager in writing prior to accessing your friend's User Data.

5. I am an engineer, and a co-worker reported encountering a bug while using the app. Can I access his account for purposes of debugging?

You may access a co-worker's User Data for purposes of debugging if they have consented to the access, and it is within the scope of your job responsibilities to de-bug. *See* Policy Rule 3(b) ("[Y]ou may Access … the User Data of a co-worker solely for purposes of de-bugging if

de-bugging is within the scope of your job responsibilities, and your co-worker has consented to the access.").

You may not access a co-worker's User Data for any purpose other than de-bugging.

6. May I access the User Data of a celebrity or public figure?

You may access the User Data of a celebrity or public figure only if necessary for your job, for example, to help a celebrity or a public figure with a customer service issue if doing so is part of your normal job responsibilities and you have been assigned their ticket.

You may not access the User Data of a celebrity or public figure out of curiosity, for any personal reason. *See* Policy Rule 2(b) ("[Y]ou **may not** Access User Data … out of curiosity … or for any other personal reason.").

7. What if I accidentally access User Data that I should not have accessed?

If you accidentally access User Data that violates any of the Policy Rules, inform your manager and privacylegal@uber.com immediately.

8. As a recruiter / hiring manager, may I check a candidate's trip history to see how much they use Uber?

No. This access is not necessary for your job responsibilities as a recruiter or hiring manager. *See* Policy Rule 1 ("You may not Access User Data, including your own, unless it is necessary to perform your job responsibilities").

This is also not permitted under Uber's User Privacy Policy.

Policy Translations

Data Access Policy Translations
English
Arabic
Portuguese (Brazil)
Bulgarian
Dutch

French (France)
German
Hindi
Italian
Japanese
Lithuanian
Polish
Romanian
Spanish (Latin America)
Spanish (Spain)
Turkish

Signature: 

Name: Bryan L. Tagaan

Date: November 19 2024

Network and Device Acceptable Use Policy

December 5, 2022

Confidential

This document is the property of Uber. It contains information that is proprietary, confidential or otherwise restricted from disclosure. “Do the right thing. Period.” is one of Uber’s cultural norms and we expect and require all entities in scope for this policy to make informed decisions regarding Uber’s information resources. Uber personnel who discover or suspect a violation of this policy must contact InfoSecPolicy-Group@uber.com.

1. Purpose

This policy defines the requirements associated with the access and use of Uber’s network, data, and information resources, regardless of whether accessed from a personal device or an Uber device.

2. Scope

For the purpose of this policy, Uber workforce and suppliers are herein referred to as Uber personnel, which means full-time and part-time employees of Uber, as well as interns, exts, temporary, contingent and casual workers, subcontractors, vendor users or consultants, or any other person engaged by Uber.

This policy applies to all Uber personnel who access or use Uber-issued devices or who access or use Uber’s network, data and/or information resources. It applies to all Uber businesses, subsidiaries, and acquired companies, unless subject to an exception or alternate policy approved by Legal.

3. Policy Requirements

3.1. General Principles

3.1.1. Uber personnel may access and use Uber’s information resources, network, and data solely for legitimate business purposes that are consistent with their roles and responsibilities.

3.1.2. Personnel must comply with all policies, procedures and requirements (including but not limited to this policy and the Data Access Policy) adopted by Security or Legal relating to access and use of Uber's network, data, and information resources.

3.1.3. Personnel may NOT circumvent or attempt to circumvent controls or restrictions implemented by Uber regarding Uber's network, data and information resources.

3.1.4. Personnel may NOT access or use the network in any way that is reasonably likely to be disruptive to the network or Uber's businesses, jeopardizes the security of Uber's network, or is not permitted under applicable laws. This includes, for example, accessing data for which the personnel is not the intended recipient, logging into a server or account that the personnel is not permitted or are not authorized to access, sniffing, port scanning, ping sweeps or floods, packet spoofing, denial of service, and forged routing information.

3.1.5. Personnel must take appropriate steps to prevent introduction of malware and other harmful materials into the network, such as by exercising caution before opening attachments or clicking on hyperlinks.

3.1.6. Uber personnel may NOT use Uber's resources, network, or data to evade legal or regulatory requirements, or law enforcement.

3.1.7. Personnel who discover misconfigurations or suspect unauthorized access or use of Uber information resources, network, and data must report these activities to security@uber.com.

3.1.8. Full-time employees of Uber or its subsidiaries who are found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Personnel who are not employees of Uber or its subsidiaries (such as contractors or contractor personnel who are granted temporary access to the network for the performance of a particular project or contract) may be subjected to revocation of the individual's right to use the network or to access Uber information resources, data, or premises and, in serious cases, the entire contract with the vendor or contractor may be terminated as a result of the personnel's violation of this policy.

3.1.9. In addition to all other requirements in this Policy, personnel working remotely must:

- Perform work activities on authorized devices
- Access systems and applications through approved mechanisms (e.g., OneLogin)
- Logically lock and physically protect devices when left unattended (e.g., devices must not be left in cars or other public areas)

3.2. Authentication Credentials

3.2.1. Personnel must protect the confidentiality and security of their authentication credentials (e.g., passwords, tokens, keys). The use of a secure password manager is encouraged. Uber's enterprise instance of LastPass is the only system authorized for storage of individual user credentials.

3.2.2. Personnel must use a unique Uber-provisioned identifier (e.g., Uber email address, Uber user ID) and password to authenticate to all Uber network, data, and information resources. Employees may NOT use the same password for more than one Uber-related account (e.g., OneLogin password must be different than Uber GitHub password, unless Uber Single Sign On (SSO) is in place). Personnel must not use their Uber-provisioned

identifier or Uber-related passwords for personal accounts, and personnel must not reuse passwords previously used for a personal account as their Uber-related authentication credentials.

3.2.3. Personnel may NOT store any plaintext credentials in internal or third-party hosted code bases. Application secrets must be stored in approved secrets management tools (e.g., uSecret, Hashicorp Vault, AWS KMS).

3.2.4. Personnel may NOT share their authentication credentials with any other person(s).

3.2.5. Personnel may NOT access the account of, or use the password of, any other personnel.

3.2.6. Personnel must immediately change authentication credentials when any unauthorized access to their account or credentials is suspected, and report any concerns to security@uber.com. In cases where application or operating system functionality does not enable personnel to change their own credentials, personnel must immediately contact it@uber.com to have their credentials changed.

3.3. Internet, Email, and Other Communications

3.3.1. Personnel should generally only access and use the network and Internet for purposes of performing work on behalf of Uber. Occasional personal use of the Internet through the network, Uber email or other authorized communication tools is allowed when such use does not:

- Interfere with Uber's operations
- Compromise functioning of the network
- Consume more than a trivial amount of resources that could otherwise be used for business purposes
- Interfere with the personnel's employment or other obligations to Uber
- Violate any laws

3.3.2. Personnel must exercise caution when opening email attachments and clicking on hyperlinks. Email attachments and hyperlinks should not be clicked if they are received from unknown sources or appear suspicious. Report all suspicious activity to security@uber.com.

3.4. Use of Cloud Services

3.4.1. For Infrastructure-as-a-Service and Platform-as-a-Service solutions (e.g., Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure):

- Appropriate teams must approve and provision accounts according to established security baselines.
- Personnel must create, receive, store, maintain or transmit Uber data on cloud services according to the Data Classification and Handling Requirements.
- Personnel must use these resources only for approved business purposes.

3.4.2. For other third party tools and SaaS applications :

- Personnel may only use enterprise accounts provisioned by Uber for approved SaaS and third party tools, including SaaS collaboration services such as Slack, Google Workplace. Unapproved SaaS applications and third party tools may not be used to perform work on behalf of Uber.

- Uber personnel may only use SaaS plugins that are in the approved SaaS and third party tools list.
- Personnel must restrict access considering the principle of least privilege and based on established criteria defined in the Access Control Policy when sharing files or folders with other collaborators.
- Data in cloud-based collaboration tools must be stored in accordance with the Data Classification and Handling Requirements. Uber reserves the right to delete or destroy any Uber data stored on Box or Google Workplace at any time.
- Uber personnel must only use SaaS solutions that have been approved by EngSec and secured in accordance with the Third Party SaaS Hardening standard.

3.4.3. Personnel are prohibited from accessing or using cloud services for any of the following activities or purposes:

- Using personal or unapproved cloud service accounts to perform job responsibilities. If it is necessary for personnel to use cloud services accounts to perform job responsibilities, only accounts provisioned by Uber for such purposes can be used.
- Sharing, uploading, or transmitting any Uber non-public data to personal cloud services accounts. Examples include, but are not limited to: Dropbox, OneDrive, iCloud Drive
- Using enterprise approved data storage and sharing platforms for personal use.
- Using any cloud-based service or platform from a third party for developing or collaborating on code containing any plaintext credential providing access to information resources that contain Uber non-public data.

3.5. Authorized Devices

3.5.1. Personnel are only permitted to access Uber's information resources, internal networks, and data using authorized devices. Authorized devices are (1) Uber devices that were issued by IT Engineering; and (2) personal phones/tablets for which Uber mobile device management (MDM) software has been installed.

3.5.2. Personnel are prohibited from bypassing, modifying, disabling, or deleting Uber-managed security controls or configurations on authorized devices (e.g., disabling anti-malware software, installing remote access software, disabling disk encryption on laptops).

3.5.3. Personnel traveling to countries on the VPN Ban List must not use their standard Uber issued laptops. Instead, they must use Uber IT issued loaner devices, which have limited functionality, when performing Uber-related business in these locations. The loaner devices must not be used on re-entry and surrendered to the IT Engineering Service Desk.

3.5.4. At Uber's discretion, access to the network and other information resources, may be terminated for a personal device in circumstances including but not limited to:

- A device not meeting Uber's hardening standards
- During leaves of absence
- When personnel transfer ownership of personal device to other people
- When personnel discard personal devices

- Upon termination of the employment relationship, and
- When Uber deems appropriate, such as in the event that personnel violate this policy.

3.5.5. Uber personnel returning from a leave of absence must notify IT@uber.com upon their return so that, where appropriate, access privileges can be reinstated.

3.5.6. Subject to any subsidies that Uber may provide at its discretion, personnel are responsible for purchasing and maintaining personal devices, and phone or data plans associated with such devices. Uber is not responsible to procure and maintain any device for personal usage apart from the benefits provided to users according to their level and region of work.

3.6. Reporting A Lost, Stolen Or Compromised Authorized Device

3.6.1. Personnel must make reasonable efforts to protect devices from being inappropriately accessed or stolen (e.g., locking computer screen, storing devices in secure, non-public areas).

3.6.2. Personnel must immediately report a lost or stolen authorized device that has been used to access Uber information resources, network, and data to security@uber.com.

3.7. Uber's Right to Access

3.7.1. To the extent permitted under applicable law, Uber reserves the right to access, collect, inspect, review, monitor, decrypt, delete, copy, remove, change, transfer, record, store, block, disclose (including within Uber and its subsidiaries, affiliates, and third parties), and otherwise process all communications, files and data stored on or transmitted using authorized devices or Uber's network, at any time and without notice.

3.7.2. In accordance with applicable law, Uber may take custody of or search Uber devices. This includes, but is not limited to, monitoring information received, stored or sent via the device, and removing information stored on Uber devices upon termination of employment with Uber.

3.7.3. Subject to applicable law, Uber may require physical access to a personal device for legitimate business purposes, such as to investigate allegations of policy violations or to implement a legal hold. Upon request, personnel must provide their personal device for inspection in a jurisdiction that makes inspection possible. Uber representatives accessing information stored on personal devices during an inspection must make reasonable efforts to limit access to only Uber's information and other information relevant to the purpose of the inspection.

3.8. Prohibitions

3.8.1. Personnel are prohibited from accessing or using Uber device or the network for any of the following activities or purposes:

- Engaging and sharing data with Third-Party Providers without following the Third-Party Information Security Policy and Data Classification and Handling Requirements.

- Using the products and services of Third-Party Providers for any purpose that is:
    - Reasonably likely to impact Uber's business, users, personnel or Uber to legal liability
    - Not permitted under applicable laws or contracts
    - Not permitted by the third party provider's terms of service
- Using any tools (e.g., program, script, command, message) with the intent to interfere with or disable another individual's session.
- Connecting to unauthorized third-party connections or making unauthorized changes to existing connection configurations.
- Downloading, copying or using for business purposes, any unlicensed content or licensed content that is not from one of Uber's preferred content licensing vendors.
- Pursuing personal profit--making or other commercial activities that are not necessary to fulfill their responsibilities or obligations to Uber.
- Downloading, copying, or using (1) unlicensed software or files; (2) licensed software or files that are not from one of Uber's preferred vendors (e.g., videos, images, movies, television programs, music, games, etc.); or (3) shareware for business purposes without prior authorization from legal. For questions regarding Uber's preferred vendors, please contact trademarks@uber.com.
- Copying, publishing, sharing or storing Uber information onto unauthorized personal or unauthorized third--party platforms and services, unless an exception is approved..
- Sending customer or user payment card or other financial account information, social security numbers, driver's license or other state, government or national identification numbers and similar types of sensitive data in the form of clear text. If you need to send such information electronically, contact security@uber.com for assistance.
- Bypassing, disabling or tampering with Uber's security controls, device configurations network, information resources, data or security logs, including security controls provided by products such as CrowdStrike and Cisco Umbrella that help protect Uber from malware and internet based threats. Visiting websites with pornographic, obscene or otherwise objectionable content unless required for a defined business need. In a case of the latter, prior written approval is required from the manager of the personnel.
- Performing malicious activities using Uber devices or Uber's network (e.g., hacking or spamming within or outside Uber's environment, introducing malicious software into the network, etc.).
- Communicating with end users or customers of Uber's services, unless required for purposes of the personnel job responsibilities.
- Engaging in any form of harassment, discrimination or other conduct prohibited by Uber's employee Business Conduct Guide.
- Creating or forwarding "Chain letters", "Ponzi", or other "Pyramid" schemes of any type.
- For personnel who have been issued an Uber email address, using any email address other than that address to conduct business on behalf of Uber. This includes but is not limited to sending business email from or to any personal or

non-essential business email address (e.g., personal Gmail address, emailing business information to friends at their office, etc.).

- Using instant messaging software (such as iMessage, Signal, WhatsApp, etc.), other than software made available by Uber, to transfer or communicate Uber information unless explicitly authorized by Engineering Security.
- Using instant messaging software made available by Uber (e.g., Slack, GChat) to transfer or communicate Tier-1 data, as defined in Uber's Data Classification and Handling standard, such as PII, payment card information, etc.
- Printing documents containing non-public Uber information, including PII.
- Copying, moving or storing non--public Uber information to local hard drives, removable drives or to a personal system unless explicitly authorized to do so in the performance of job responsibilities. If expressly authorized to store non-public Uber information onto removable media, it must be documented and meet Uber's Data Classification and Handling Requirements.
- Transferring any Uber confidential information outside of Uber's network, except where necessary to perform job responsibilities.

4. Exceptions

In situations where the requirements of this policy cannot be effectively addressed, an exception request must be submitted using this Exception Form. All exception requests will be assessed and approved or rejected based upon Uber's Information Security Exception Management Process.

5. Enforcement

Violations are subject to notification of non-compliance and may result in disciplinary actions on Uber personnel, up to and including termination.

6. Responsibility Matrix

Role	*Responsibility*
Uber Personnel	[All Requirements] - Access or use Uber's network, data and/or information resources, in accordance with this policy

7. Related Documents and Resources

- Information Security Policy
- Access Control Policy
- Data Classification and Handling Requirements
- Third-Party Information Security Policy
- AWS Security Baseline for AWS Accounts
- Business Conduct Guide

- Approved SaaS and Third Party Tools Standard
- Third Party SaaS Hardening standard

Terms and Definitions

Term	***Description***
Document Owner	Entity (Team and/or Personnel) of Uber, that controls this document and is accountable for governance of the "policy management lifecycle," which includes creation, review, approval, communication, exceptions, compliance, maintenance and retirement.
Uber Personnel	Full-time and part-time employees of Uber and Uber's subsidiaries, as well as interns, exts, temporary, contingent and casual workers, subcontractors, vendor users or consultants, or any other person engaged by Uber.
Third-Party Provider	Vendors, suppliers, service providers, consultants, partners, joint ventures, counterparties, cloud services providers, SaaS/PaaS services providers, website hosting platforms or any other organizations who engage with Uber in the delivery of products and services, directly or as subcontractors.
Information Resources	Systems, devices, and software that are used in operation of Uber's business and facilitate the creation, maintenance, storage, or use of information. Examples of information resources include, but are not limited to: - Desktops & laptops - Servers including hardware, firmware, OS and associated infrastructure (e.g., rack) - Third-party cloud-based services or platforms for which Uber has the technical ability and contractual authority to configure security settings (e.g., Amazon Web Services Simple Storage Service) - Monitors, printers, and scanners - Phones other mobile devices and tablets - Removable media - Network infrastructure devices e.g. switches, routers, firewalls including software-based tooling - Application software and services, system software, firmware, development tools, utilities - Embedded systems - Security tools such as IDS/IPS, anti-malware solutions, endpoint protection
Mobile Device Management (MDM) Solution	MDM is software that enables secure access to the network, and that configures and provisions corporate applications on mobile devices such as work email and calendar within a partitioned area of the device.

Authentication Credentials	Combination of the user ID or account ID plus the authentication factor(s) used to authenticate an individual, device, or process.
Authorized Devices	(1) Uber IT issued devices and (2) personal phones/tablets for which MDM has been installed.
Uber Device	Any device (e.g., laptop, mobile phone, media) used by personnel that has been issued by Uber.
Personal Device	Any device (e.g., laptop, mobile phone, media) used by personnel that was not issued by Uber.
Password Manager	Software application or a hardware device that is used to store and manage passwords.
Principle of Least Privilege	Restricting access to the minimum level of information and resources that are necessary to perform job responsibilities.
Unlicensed Software	Software for which no license or permission has been obtained or software for which the number of authorized copies or users has been exceeded.
Unlicensed Software Use	Downloading, sharing, selling, or installing multiple copies of licensed software. Unlicensed software use also includes license infringement (i.e.,installing a piece of software more times than the license permits).
Malicious Software	Any software that brings harm to a computer system (e.g., worms, viruses, trojans, spyware, adware and rootkits).
Local Hard Drive	Hard drive that is physically installed inside of or connected to a computer and is not part of another computer on a network.
Removable Media	Any type of storage device that can be removed from a computer while the system is running (e.g., USB, CD, etc.)
Instant Messaging Software	Communication technologies used for text-based communication between two or more participants over the Internet or other types of networks.
Changes	Modifications to information resources performed by Uber personnel.
Uber Data	Data collected or retained by or on behalf of Uber.
VPN Ban List Countries	Belarus, North Korea, Turkmenistan, China, Iraq, Iran, Oman, Russia, United Arab Emirates, and Turkey

Unauthorized Third-Party Connection	A connection made with an entity external to Uber that has not been approved by the Third-Party Risk Management Team

Document Control

Document Name	Network and Device Acceptable Use Policy		
Document Source	Information Security Policy		
Document Owner	Security Assurance		
Creation Date	12/10/2018	***Effective Date***	January 15, 2019
Distribution List	***Document Sent To***		***Purpose***
	Engineering Security		For Creation
	Privacy Legal		For Review
	Engineering Security		For Approval
Help	For questions and feedback regarding this policy and Uber's information security policies in general, please contact InfoSecPolicy-Group@uber.com.		
Policy Change Requests	For suggested changes to the contents of this policy, please submit suggestions through the IS Policy Change Request Form		

Version History

Version #	***Date Modified***	***Modified By***	***Changes Made***
1.0	12/10/2018	Alex Landeta	Initial Publication
1.0	01/02/2019	Rafa Gutierrez	Initial Draft Reviewed and Finalized
1.0	01/10/2019	Derek Care	Initial Draft Reviewed and Finalized

1.0	01/15/2019	Shawnee Delaney and Stella Chamarelli	Initial Draft Reviewed and Finalized
1.1	02/11/2019	Alex Landeta	Modified use of USB devices
1.2	07/24/2019	Alex Landeta	Policy Change Request Link Added Duplicative content removed
1.3	09/10/2020	Rachid Macer	Annual Review
1.4	8/30/2021	Alex Landeta	Annual Review
1.5	9/09/2022	Rocky Kurien	Annual review
1.6	10/14/2022	Ollie Gallardo and Erk Gomez	Section 3.5: Scoped authorized personal devices to phones/tablets, added other language for further clarification. Removed requirement for informing IT when transferring/selling employee owned personal devices. Section 3.2.1: Adjusted language to prohibit non-authorized password managers. Section 3.2.4: Added Hashicorp Vault as a secrets storage solution for Uber. Section 3.4.1: Provided more concrete scoping Section 3.4.2: Added language for additional clarity. Section 3.4.3: Added cloud storage examples. Section 3.6: Removed unnecessary language Section 3.8.1: Revised examples and language in relation to instant messaging Section 7: Added references to hardening standards Terms & Definitions: added more explicit working around authorized devices.

Approval History

Version #	*Date Approved*	*Approved By*	*Approval Signature*
1.0	January 15, 2019	Melissa Bishop	Melissa Bishop
1.1	February 11, 2019	Melissa Bishop	Melissa Bishop
1.2	September 13, 2019	Melissa Bishop	Melissa Bishop
1.3	September 24, 2020	Melissa Bishop	Melissa Bishop
1.4	September 16, 2021	Melissa Bishop	Melissa Bishop
1.5	September 09,2022	Rahul Goel	Rahul Goel
1.6	October 14, 2022	Daniel Steyn	Daniel Steyn

Acknowledged by:

Signature

Bryan L. Tagaan

Printed name

November 19, 2024

Date

Dear Uber EXT:

On October 25, 2018, Uber entered into a settlement agreement with the Federal Trade Commission, the regulatory agency responsible for U.S. consumer rights protections. The agreement will affect how Uber processes and protects U.S. user personal information.

Why this is important:
Earning and maintaining users' trust starts with honoring Uber's promises to them. This means that when we represent Uber to the public, we must be accurate about any claims we make about Uber's data privacy and data security practices, specifically about how Uber or we access, use, share, and protect user personal information. This affects statements Uber makes in advertisements, other marketing and promotional materials, blog posts, press interviews, presentations, and community operations communications to users.

It also affects Uber's and our practices internally because these practices must be consistent with any external claims Uber has made. In addition, Uber must engage in "privacy by design" and think about privacy risks and practices *before* engaging in any new data practices or changing its data practices.

How this affects you
Because you may have access to U.S. user personal information on behalf of Uber, you are required to receive and acknowledge a copy of the settlement agreement prior to beginning your role.

Acknowledged by:

signature

Bryan L. Tagaan
printed name

Date: November 19, 2024

1523054

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Joseph J. Simons, Chairman**
Noah Joshua Phillips
Rohit Chopra
Rebecca Kelly Slaughter
Christine S. Wilson

In the Matter of **Uber Technologies, Inc.,** **a corporation.**	**DECISION AND ORDER** **DOCKET NO. C-4662**

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondent a draft Complaint. Respondent and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement").

The Commission determined that it had reason to believe that Respondent had violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered the comments received from interested persons pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34, and the recommendations of its staff.

BCP then prepared and furnished to Respondent a revised draft Complaint that BCP proposed to present to the Commission for its consideration. Respondent and BCP executed a revised Consent Agreement containing (1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and (2) waivers and other provisions as required by the Commission's Rules.

The Commission thereafter reconsidered the matter and again determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, as stated in the revised Complaint, and that the revised Complaint should issue stating the Commission's charges in that respect. The Commission withdrew its acceptance of the original Consent Agreement and placed the revised Consent Agreement on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered the comments received from interested persons pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34, and the recommendations of its staff. Now, in further conformity with the procedures prescribed

in Commission Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. Respondent, Uber Technologies, Inc., is a Delaware corporation with its principal office or place of business at 1455 Market St. #400, San Francisco, California 94103.

2. The Commission has jurisdiction over the subject matter of this proceeding and over Respondent, and the proceeding is in the public interest.

ORDER

Definitions

For purposes of this Order, the following definitions apply:

A. "Covered Incident" means any instance in which any United States federal, state, or local law or regulation requires Respondent to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by Respondent from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization.

B. "Personal Information" means individually identifiable information collected or received, directly or indirectly, by Respondent from or about an individual consumer, including: (1) a first and last name; (2) a physical address; (3) an email address; (4) a telephone number; (5) a Social Security number; (6) a driver's license or other government-issued identification number; (7) a financial institution account number; (8) persistent identifiers associated with a particular consumer or device; or (9) precise geo-location data of an individual or mobile device, including GPS-based, WiFi-based, or cell-based location information.

C. "Respondent" means Uber Technologies, Inc. and its successors and assigns.

Provisions

I. Prohibition Against Misrepresentations

IT IS ORDERED that Respondent and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service must not misrepresent in any manner, expressly or by implication:

A. the extent to which Respondent monitors or audits internal access to consumers' Personal Information; or

B. the extent to which Respondent protects the privacy, confidentiality, security, or integrity of any Personal Information.

II. Mandated Privacy Program

IT IS FURTHER ORDERED that Respondent must, no later than the effective date of this Order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of Personal Information. Such program, the content and implementation of which must be documented in writing, must contain controls and procedures appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the Personal Information, including:

A. the designation of an employee or employees to coordinate and be responsible for the privacy program;

B. the identification of reasonably foreseeable risks, both internal and external, that could result in Respondent's unauthorized collection, use, or disclosure of Personal Information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including: (1) employee training and management, including training on the requirements of this Order; (2) product design, development, and research; (3) secure software design, development, and testing, including access key and secret key management and secure cloud storage; (4) review, assessment, and response to third-party security vulnerability reports, including through a "bug bounty" or similar program; and (5) prevention, detection, and response to attacks, intrusions, or systems failures;

C. the design and implementation of reasonable controls and procedures to address such risks and regular testing or monitoring of the effectiveness of those controls and procedures;

D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of Personal Information they receive from Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such Personal Information; and

E. the evaluation and adjustment of Respondent's privacy program in light of the results of the testing and monitoring required by sub-provision C, any changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the privacy program.

III. Privacy Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with its compliance with the Provision of this Order titled Mandated Privacy Program, Respondent must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be completed by a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. An individual qualified to prepare such Assessments must have a minimum of 3 years of

experience in the field of privacy and data protection. All individuals selected to complete such Assessments must be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, in his or her sole discretion. Any decision not to approve an individual selected to conduct such Assessments must be accompanied by a writing setting forth in detail the reasons for denying such approval.

B. The reporting period for the Assessments must cover: (1) the first 180 days after the issuance date of the Order for the initial Assessment, and (2) each 2-year period thereafter for 20 years after the issuance date of the Order for the biennial Assessments.

C. Each Assessment must:

1. set forth the specific privacy controls that Respondent has implemented and maintained during the reporting period;

2. explain how such privacy controls are appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the Personal Information;

3. explain how the privacy controls that have been implemented meet or exceed the protections required by the Provision of this Order titled Mandated Privacy Program; and

4. certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of Personal Information and that the controls have so operated throughout the reporting period.

D. Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies. Respondent must provide each Assessment to the Commission within 10 days after the Assessment has been completed. Respondent must notify the Commission of any portions of the Assessment containing trade secrets, commercial or financial information, or information about a consumer or other third party, for which confidential treatment is requested pursuant to the Commission's procedures concerning public disclosure set forth in 15 U.S.C. § 46(f) and 16 C.F.R. § 4.10.

IV. Covered Incident Reports

IT IS FURTHER ORDERED that Respondent, within a reasonable time after the date of Respondent's discovery of a Covered Incident, but in any event no later than 10 days after the date Respondent first notifies any U.S. federal, state, or local government entity of the Covered Incident, must submit a report to the Commission:

A. The report must include, to the extent possible:

1. the date, estimated date, or estimated date range when the Covered Incident occurred;

2. a description of the facts relating to the Covered Incident, including the causes and scope of the Covered Incident, if known;

3. a description of each type of information that triggered the notification obligation to the U.S. federal, state, or local government entity;

4. the number of consumers whose information triggered the notification obligation to the U.S. federal, state, or local government entity;

5. the acts that Respondent has taken to date to remediate the Covered Incident and protect Personal Information from further exposure or access; and

6. a representative copy of each materially different notice required by U.S. federal, state, or local law or regulation and sent by Respondent to consumers or to any U.S. federal, state, or local government entity.

B. Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re: Uber Technologies, Inc., File No. 1523054."

V. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

A. Respondent, within 10 days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For 20 years after the issuance date of this Order, Respondent must deliver, or for contingent workers, cause to be delivered, a copy of this Order to (1) all principals, officers, directors, and LLC managers and members; (2) all employees, agents, and representatives who participate in conduct related to the subject matter of the Order, including all employees, agents, and representatives who regularly access Personal Information; and (3) any business entity resulting from any change in structure as set forth in the Provision of this Order titled Compliance Report and Notices. Delivery must occur within 10 days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which Respondent delivered, or caused to be delivered, a copy of this Order, Respondent must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

VI. Compliance Report and Notices

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

A. One year after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which:

   1. Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, that representatives of the Commission may use to communicate with Respondent; (b) identify all of Respondent's subsidiaries that are registered as business entities in any state of the United States by all of their names, primary telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the products and services offered by each business and the Personal Information each business collects, maintains, transfers or stores; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes Respondent made to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

B. Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following: (1) any designated point of contact; or (2) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within 14 days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re: Uber Technologies, Inc., File No. 1523054."

VII. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for 20 years after the issuance date of the Order, and retain each such record for 5 years, unless otherwise specified below. Specifically, Respondent must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold;

B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an independent contractor, employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. Records of all consumer complaints directed at Respondent, or forwarded to Respondent by a third party, concerning the subject matter of the Order, and any response;

D. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission;

E. A copy of each widely disseminated representation by Respondent that describes the extent to which Respondent maintains or protects the privacy, security, and confidentiality of Personal Information, including any representation concerning a change in Respondent's practices with respect to the privacy, security, and confidentiality of Personal Information;

F. For 5 years after the date of preparation of each Assessment required by this Order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by such Assessment;

G. For 5 years from the date created or received, reports received by Respondent from individuals or entities that seek payment, rewards, or recognition through a "bug bounty" or similar program for reporting a security vulnerability that relates to potential or actual access to or acquisition of Personal Information, and records sufficient to show Respondent's review, assessment of, and response to any such reports;

H. For 5 years from the date created or received, copies of all subpoenas and other communications with law enforcement, if such communications relate to Respondent's compliance with this Order; and

I. For 5 years from the date created or received, all records, whether prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent's compliance with this Order.

VIII. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

A. Within 10 days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

IX. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate on October 25, 2038, or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than 20 years;

B. This Order's application to a Respondent that is not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any Provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission, Commissioner Wilson not participating.

Donald S. Clark
Secretary

SEAL:
ISSUED: October 25, 2018