PRIVACY AND COOKIE POLICY

1. Introduction

Reply S.p.A. with registered office in Corso Francia n. 110, Turin, Italy, (hereinafter "**Reply**") and Reply group companies (jointly defined as "**We**", "**Us**" or "**Our**"), as identified below, respect your privacy and are committed to protecting it through Our compliance with this Privacy and Cookie Policy ("**Privacy and Cookie Policy**").

This Privacy and Cookie Policy covers the processing of personal data carried out through owl.reply.com ("**Site**") concerning the following categories of users:

- prospective suppliers (in case of natural person and self-employed individuals) interested in opportunities with Reply Group companies, including consultants and employees as well as legal representatives, shareholders, directors, delegates, officers and any other persons with representation and/or management and/or control powers of the prospective supplier, which access the Site as external users ("**Prospective Supplier/s**");
- current and former suppliers (in case of natural persons and self-employed individuals), including consultants and employees as well as legal representatives, shareholders, directors, delegates, officers and any other persons with representation and/or management and/or control powers of the supplier, which access the Site as external users in the context of their contractual relationship with the relevant Reply Group company, as defined below ("**Supplier/s**");
- Reply and Reply group companies' employees who access the Site in the context of their job duties and tasks as internal users ("**Reply Users**");

Reply Users, Prospective Suppliers and Suppliers are hereinafter jointly referred to as "**Data Subjects**".

Depending on the data subject location, additional terms and conditions concerning personal data protection may apply. These additional terms ("**Supplementary Notice**") are incorporated into Section 13 below, and should be read alongside, this Privacy and Cookie Policy by reference to the applicable jurisdiction. These terms are occasionally updated to comply with specific legal requirements and prevail over this Privacy and Cookie Policy in case of contrast.

2. Data Controller identity and contact details

The Data Controller for the processing activities related to Data Subjects is Reply.

The Data Controller for the processing activities related to Suppliers is the specific Reply Group company which holds the contractual relationship with the Supplier ("**Company**"). The Company name and contact details of the relevant Company acting as Data Controller are specified within the agreement entered into by the Supplier with such Company ("**Agreement**").

Reply and each Company act as autonomous data controllers with regards to the processing of Data Subjects' personal data described in this Privacy and Cookie Policy.

DPO contact details

Data Protection Officers (DPO) for Our European Companies, depending on the location of their registered office, can be contacted at the following addresses:

- Italy: dpo.it@reply.it
- Germany: dpo.de@reply.de
- United Kingdom and France: dpo.uk@reply.com

3. Source of data processed

3.1. Personal data relating to the Prospective Suppliers and Suppliers are collected directly from them during their Site account registration and set-up, from publicly available sources and from the company/entity which the Data Subject belongs to during the negotiations necessary for the evaluation of their proposed services, their assessment, and the potential execution and termination of the Agreement for the supply of services and/or goods or of the different commercial relationship established with the Company.

3.2. Personal data relating to Reply Users is collected directly from the latter at the time of hiring and/or during the course of the employment or collaboration relationship with Reply and/or the relevant Reply group Company.

3.3. Personal data relating to Data Subjects are jointly referred to as "**Data**".

4. Categories of data processed

4.1. Reply processes Data collected during Site navigation such as IP address and other parameters related to the browser and operating system used by Data Subjects when they access and browse the Site.

4.2. Reply may process the following Data:

a) personal details, including name and surname, identity document details and the role held in the company/entity to which the Data Subject belongs;

b) the contact details, including the address, telephone number and e-mail address;

c) in the event that the Prospective Supplier is a natural person, the company name, the office's main and secondary (if any) addresses, the VAT number and/or tax code, the details of the bank account(s) of the Data Subject;

4.3. With reference to Reply Users, Reply processes the following categories of personal data:

a) personal details, including name and surname;

b) job details, including role held within Reply and/or the Company;

c) contact details, including business e-mail address.

4.4. Furthermore, the relevant Company processes – in addition to the data listed under letters a) to c) of Section 4.2. above - the following additional Data of Suppliers in the context of the execution of the contractual relationship:

d) information on the mobile device used by the Supplier's employees/consultants to enforce strong authentication mechanism on specific Reply services (e.g. the Reply VPN); and

e) any further Data Subject's personal data that may be collected during the negotiation and potential execution, performance and termination of the Agreement with the Company.

4.5. Should the Prospective Supplier and/or Supplier provide personal data relating to other individuals (including, without limitation, any of their own employees or other personnel), the Prospective Supplier and/or Supplier acknowledges, represents and warrants that it will provide such third party personal data only after:

a) having informed with due advance the concerned persons of the communication of their personal data to Us; and

b) having relied on an appropriate and valid legal basis for the communication of their personal data for the purposes of this Privacy and Cookie Policy.

4.6. Data Subjects shall under no circumstances provide Us with special categories of personal data either relating to them or any other individual (e.g. personal data revealing: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric information and information on the health status or sexual orientation). To the extent that any special categories of personal data is provided to Us at any time, Data Subjects give and, where applicable, acknowledge that any such other individuals whose special categories of personal data was provided to Us have given, their explicit consent for such data to be communicated to Us. All references to special categories of personal data in this policy shall be construed in accordance with the GDPR.

5. Data processing purposes and legal grounds for the processing

5.1. Reply processes Data related to Data Subjects to allow them to access and browse the Site. In particular, Reply processes such Data to enable the creation of an account for the Site and carry out maintenance activities to guarantee the proper functioning of the Site. In the cases above, the legal basis for the processing is the execution of pre-contractual and/or contractual activities (jointly referred to as "**Access and Maintenance Purposes**").

5.2. Reply processes Data related to Prospective Suppliers to perform an evaluation of their services/capabilities proposed via the Site or other communication channels such as contact forms or e-mail. When Prospective Suppliers use a Reply contact form, their Data may be stored in the Reply ticketing system for backup and request management purposes. In the cases above, the legal basis for the processing is the execution of the pre-contractual activities (jointly referred to as "**Pre-Contractual Purposes**").

5.3. The Company processes the Data for the negotiation, and the potential conclusion, execution and termination of the Agreement between the Supplier and the Company. In this case the legal basis for the processing is the performance of the contract entered into with between the Company and the Supplier (jointly referred to as "**Contractual Purposes**").

5.4. We process the Data to comply with the obligations arising from the applicable laws and regulations (e.g. administrative-accounting obligations), including the communication to competent authorities and supervisory bodies and to comply with requests coming from them. In this case the legal basis for the processing is the need to fulfil a legal obligation to which We are subject (jointly referred to as "**Legal Obligation Purposes**").

5.5. The Company and/or Reply process the Data for enforcing / defending Our rights in court and to perform activities that are functional to transfers of assets, branch of business, acquisitions, mergers, divisions or other corporate operations. The Company and/or Reply also process the Data to manage Our IT resources, including infrastructure, websites and technological equipment, to ensure service continuity and guarantee IT security (e.g. to prevent cyber-attacks or perform checks in case of attacks) and verify Suppliers' compliance with the requirements provided by Our corporate policies. Furthermore, Reply can transfer the Data to other Companies to enable them to engage Suppliers. In the cases above the legal basis for the processing is Our legitimate interest (jointly referred to as "**Legitimate Interest Purposes**").

5.6. The provision of Data is necessary with reference to the Access and Maintenance Purposes, Contractual, Pre-Contractual and Legal Obligation Purposes in order to allow access and the proper functioning of the Site, perform the evaluation activities and negotiate, stipulate, execute and/or terminate the Agreement between the Company and the Data Subject, as well as in order to comply with the provisions of the applicable legislation. Failure to provide the Data for such purposes shall result in the impossibility for Reply to allow access and maintain the Site, evaluate the Prospective Suppliers and enter into an Agreement with them or execute the Agreement in place with the Suppliers.

5.7. Processing for the Legitimate Interest Purposes is carried out in pursuit of Our legitimate interests which are adequately balanced with the legitimate interest of the Data Subjects, since the Data processing activity is limited to what is strictly necessary for the exercise or defense of Our rights and performance of the economic operations described above. The processing for Legitimate Interest Purposes is not mandatory and the Data Subject may object to such processing as indicated in Section 11.3 below of this Privacy and Cookie Policy. Should the Data Subject object to such processing, his or her Data may not be used for the aforementioned purpose, unless Reply and/or the relevant Company has a compelling legitimate ground for the processing that overrides the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defense of a right in a court of law.

5.8. If you have any questions or would like more information about the legal basis for collecting your personal information, please contact Reply and/or the relevant Company at supplier.privacy@reply.com.

6. Data retention period

6.1. Data will be processed for the period of time strictly necessary for the pursuit of the purposes set out in this Privacy and Cookie Policy. In any case, Data will be stored for no longer than the retention periods detailed below.

6.2. Data collected and processed for Access and Maintenance Purposes are stored for until the navigation session has terminated or for the period indicated under Section 6.6 below, unless a longer retention is required for any litigation, requests by the competent authorities, or pursuant to applicable legislation.

6.3. Prospective Suppliers' Data collected for the Pre-Contractual purposes are stored for up to 12 months upon receiving their application.

6.4. In the event of a positive outcome of the evaluation and contractual negotiations, Supplier's Data are retained for the entire duration of the Agreement and for 10 years following the Agreement's termination; in the event of a negative outcome of contractual negotiations, Personal Data will be deleted at the end of the negotiation phase.

6.5. Data collected for the Legal Obligation Purposes are retained for the duration prescribed for each type of personal data by the applicable laws, and in any case for up to 10 years after the collection.

6.6. Data collected for the Legitimate Interest Purposes are retained for the entire duration of the Agreement and for the following 10 years, in the event the Data was necessary to protect and enforce Our rights in any legal disputes.

6.7. Supplier's employees/consultants Data collected and used to enforce strong authentication mechanism to Reply services are stored for 6 months after the strong authentication mobile app and user is disenrolled from the Reply strong authentication service.

6.8. Once the above storage terms have elapsed, Data will be destroyed or anonymized, save in cases for which Data shall be further retained to respond or to file legal actions, upon request of the competent authorities or in compliance with the applicable laws.

7. Third parties and data recipients

7.1. To pursue the above-mentioned purposes, Data may be communicated to the following third parties or data recipients:

a) personnel belonging to Reply and/or the relevant Company which has been authorized and instructed to process Data or the subjects indicated below as data processors, within the scope of their respective duties and within the limits established by the applicable law;

b) providers of support services, as well as of assistance or advice, to the relevant Reply group company, such as, by way of example but not limited to, legal, administrative and tax consultants, banks for the management of collections and payments arising from the execution of the contract between the relevant Company

and the Data Subject or the company/entity to which the latter belongs, auditing companies, suppliers of technological services, as autonomous data controllers or data processors;

c) sub-providers and/or sub-contractors engaged in activities connected to the execution of the Agreement between the relevant Company and the Data Subject or the company/entity to which the latter belongs, in their quality as data processors;

d) public bodies and/or judicial and/or control authorities, whose right to access the Data is provided for by the applicable legislation, acting as independent data controllers; and

e) other companies belonging to the Reply group and/or subjects transferring a company or business, companies resulting from possible mergers or any other transformation involving the relevant Company, acting as autonomous data controllers.

7.2. Data of Prospective Suppliers which have successfully overcome the evaluation may be shared by Reply to other Companies which are interested in the service provided by the Prospective Supplier.

8. Data security

8.1. We process the Data for the purposes above through adequate paper and electronic means and implement appropriate measures to ensure Data confidentiality and security. In particular, We adopt appropriate organizational and technical measures to protect Data against loss, theft, as well as unauthorized use, disclosure or modification.

8.2. The following is a non-exhaustive list of the measures adopted by us to protect Data:

a) every access to the Site is secured by login and password credentials, which must be periodically changed to limit the risk of unauthorized access;

b) all Site communications are protected by encryption;

c) all software systems supporting the Site are set up with state-of-the-art data protection technology.

9. Data transfers

9.1. Both EU/UK and non-EU/UK Suppliers and/or Prospective Suppliers' Data could be accessed by Reply Group Companies which are based within the EU/UK (see "Offices" at www.reply.com).

9.2. In case of transfers from EU/UK to countries not considered adequate by the European Commission/UK Data Protection Authority (as applicable), We have put in place appropriate and suitable safeguards to protect the Data. Accordingly, Data Subjects' Data are transferred in compliance with the requirements and the obligations provided by applicable data protection laws, such as an adequacy decision or standard contractual clauses adopted by the European Commission/UK Data Protection Authority (as applicable).

9.3. In particular, in order to transfer the Data outside the EU/UK, We will enter into the appropriate module of the Standard Contractual Clauses issued by the European Commission on 4 June 2021 with the relevant data importer and adopt any supplementary measure required as a consequence of the decision of the European Court of Justice C-311/18.

9.4. If the Data Subjects wish to have more information on such transfers, he/she may at any time send an email to supplier.privacy@reply.com.

10. Cookies

10.1. The Site, which is managed by Reply, uses cookies, which are small files with configuration settings, to help Us make the Site more user-friendly, effective and

secure. Cookies are also used to implement certain user functions. In particular, cookies contain information sent by a web server to the visitor/user's Internet browser and automatically stored by the latter on the device (personal computer, tablet, smartphone, etc.) and automatically sent back to the server each time the Site is accessed.

10.2. Cookies can be distinguished based on the following criteria:

a) based on who manages cookies:
   (i) **first party cookies**: these are cookies installed directly by a data controller (or processors acting on its behalf) through a website;
   (ii) **third party cookies**: these are cookies installed through a website by third parties other than the data controller and processed by such third-parties for purposes they solely determine;

b) based on the time they remain enabled:
   (i) **session cookies**: these cookies store the necessary information during the browsing session and are deleted immediately after the session expires, i.e. when the browser is closed;
   (ii) **persistent cookies**: these cookies are stored on the user's hard disk and the website reads them each time the same user visits the same website. A persistent cookie has a specific expiry date, after which it will stop working;

c) based on their purpose:
   (i) **technical cookies**: these cookies are necessary to allow a user to browse a site and to benefit from its functionalities. If strictly necessary for the use of a website, these cookies do not require the user's prior consent and cannot be switched off. Without these cookies some services or functions could not be provided and the browsing of the website would not be easy and functional;
   (ii) **analytics cookies**: these cookies are used to obtain statistical information, in an aggregate manner or not, on the number of users accessing a website and about how the website is used. Where required by the applicable laws, if the user does not consent to these types of cookies, the data controller will not be able to improve the website based on information from the user's visit;
   (iii) **profiling cookies**: these cookies are used to trace a user's profile in order to display advertisements on the website targeted on the basis of the user's interests, tastes and consumption habits. If a user does not consent to these types of cookies, he/she will experience less targeted advertising (but not less advertising overall).

10.3. The Data Subjects navigating the Site can choose the browser or the privacy settings of their devices so that they are informed about the setting of cookies and only allow cookies in individual cases. They can also exclude the acceptance of cookies for certain cases or generally and activate the automatic deletion of cookies when closing the browser. However please note that by deleting or blocking the technical cookies, the Site (or its functionalities) may not work properly or efficiently.

10.4. The Data Subjects can learn more about cookies and how to block cookies on different types of browsers by visiting https://www.allaboutcookies.org. In particular, more information on how to enable and disable cookies can be found here https://allaboutcookies.org/how-to-manage-cookies.

10.5. This Site implements technical cookies only. Technical cookies are used for the sole purpose of allowing the Data Subjects to visit the Site. They can be further divided into:
   (i) **necessary cookies**: these cookies guarantee the ordinary browsing and use of a website, allowing, for instance, to book an appointment or to authenticate for accessing reserved areas. Therefore, they are strictly necessary for the browsing and use of a website and, thus, do not require the website user's consent. These are generally session cookies, which are automatically deleted when closing the browser;
   (ii) **functional cookies**: these cookies allow website users to browse a website according to a set of selected criteria (for instance, the language or country of

origin) in order to improve the service provided. Therefore, without these cookies some of the services and functionalities provided on the Site may not function properly. These are persistent cookies, which remain on the computer in use even after the browser is closed, until the expiry date provided for each cookie (typically from two months to two years) or the user deletes them.

11. Data Subjects' rights

11.1. Notwithstanding the possibility for the Data Subjects not to provide their Data, if the processing of Data Subjects' personal data is subject to EU data protection laws, they can exercise the following rights free of charge and at any given time:

a) obtain confirmation of the existence of Data relating to them;

b) know the origin of the Data, the purposes of the processing and its methods, as well as the logic applied to the processing carried out by electronic means;

c) verify the accuracy of Data and request its integration, update or amendment;

d) request the erasure, anonymisation or restriction of the processing of Data processed in breach of the applicable laws, and object, on legitimate grounds, to the processing of Data;

e) withdraw previously given consents, if any;

f) request to limit the processing of the Data where (i) Data Subjects contest the accuracy of the personal data until the relevant Company has taken sufficient steps to correct or verify its accuracy; (ii) the processing is unlawful but the Data Subjects do not want Us to erase the Data; (iii) We no longer need the Data for the purposes of the processing, but the Data Subjects require them for the establishment, exercise or defense of legal claims; or (iv) Data Subjects have objected to processing justified on legitimate interests, pending verification as to whether We have compelling legitimate grounds to continue the processing;

g) object to the processing of the Data for the processing activities based on Our legitimate interest;

h) request the erasure of the Data without undue delay; and

i) obtain Data portability to receive the Data that had been previously supplied to Us in a structured, common use and readable format.

11.2. If Legislative Decree No. 196/2003 as subsequently amended and supplemented by Legislative Decree no. 101/2018 ("**Italian Privacy Code**") applies to the processing of Data Subject's Data, in case of Data Subject's death, the aforesaid rights relating to their Data may be exercised by anyone who has a personal interest, or acts to protect the Data Subject as its representative, or for family reasons worthy of protection pursuant to article 2-*terdecies* of the Italian Privacy Code. Data Subjects may expressly prohibit the exercise by its assignees of some of the rights above by written notice to be sent to Reply and/or relevant Company as described below, without prejudice to their right to withdraw or modify such expressed intention later on according to the same procedure.

11.3. Requests for the exercise of your rights may be made in writing to Reply and/or relevant Company acting as Data Controller at the contact details specified within the Agreement or at the following e-mail address supplier.privacy@reply.com.

11.4. The Data Subjects have also the right to lodge a complaint to the relevant Supervisory Authority in particular, in the Member State in which he/she has habitual residence or place of work, or in the place where the alleged infringement occurred.

12.CHANGES AND UPDATES

12.1. This Privacy and Cookie Policy is valid from the date of effectiveness provided at the top. However, the Privacy and Cookie Policy may subsequently be updated or integrated, from time to time, also as consequence of possible subsequent amendments and/or integrations of the applicable laws. Changes will be notified in advance and Data Subjects will be able to consult the constantly updated version of this Privacy and Cookie Policy on the Site.

13. SUPPLEMENTARY NOTICE

13.1. PEOPLE'S REPUBLIC OF CHINA

This Section 13.1 applies if the Data Subject is located within the People's Republic of China ("**PRC**").

13.1.1. Processing of Sensitive Personal Data

a) Under applicable law (including the Personal Information Protection Law of the PRC ("**PIPL**")), Sensitive Personal Data is Data that, once leaked or illegally used, may easily lead to the infringement of the personal dignity of a natural person or may endanger his personal safety or property, including information such as biometrics, religious belief, specific identity, medical health status, financial accounts, and the person's whereabouts, as well as the Data of a minor under the age of 14 years.
b) We will in principle not process Sensitive Personal Data. If Sensitive Personal Data will be processed, We will notify the Data Subject about the processing, and obtain separate consent if applicable.

13.1.2. Data Processing Purposes and Legal Basis

- We process the Data for Access and Maintenance Purposes (see defined above);
- We process the Data Pre-Contractual Purposes (see defined above);
- We process the Data for Contractual Purposes (see defined above);
- We process the Data for Legal Obligation Purposes (see defined above);
- We process the Data for Legitimate Interest Purposes (see defined above).

We will only process the Data where We have a legal basis for doing so. In many cases, We will obtain consent from Data Subjects prior to processing their Data, including a separate consent where required by applicable law, as the legal basis for the processing. Other legal bases that We may rely on to process the Data, including where consent may not be required, may include:

a) the processing is necessary for the conclusion or performance of a contract, or where it is necessary for carrying out human resources management under an employment policy legally established or a collective contract legally concluded;
b) the processing is necessary for us to perform our statutory duties or obligations;
c) the processing is necessary for us to respond to a public health emergency, or for protecting the life, health or property security of a natural person in the case of an emergency;
d) The processing is necessary for any other circumstances as provided by law or administrative regulations.

13.1.3. International Data Transfers

The Data are accessed and processed by Reply Group Companies that are based outside of the PRC (see "Offices" at www.reply.com). We have put in place appropriate and suitable safeguards to protect the Data during international transfer. Accordingly, Data Subjects' Data are transferred in compliance with the requirements and the obligations provided by applicable data protection laws.

13.1.4. Data Subjects' Rights

Data Subjects that reside in the PRC may exercise the following rights free of charge and at any time by contacting us via the information set forth above:

a) obtain confirmation of the existence of Data relating to them;
b) know and to be explained with the origin of the Data, the purposes of the processing and its methods, as well as the logic applied to the processing carried out by electronic means;
c) verify the accuracy of the Data and request its integration, update or amendment;
d) request the erasure, anonymisation or restriction of the processing of Data processed in breach of the applicable laws, and object, on legitimate grounds, to the processing of the Data;
e) withdraw previously given consents, if any;
f) request to limit the processing of the Data where (i) Data Subjects contest the accuracy of the Data until We have taken sufficient steps to correct or verify its accuracy; (ii) the processing is unlawful but the Data Subjects do not want Us to erase the Data; (iii) We no longer need the Data for the purposes of the processing, but the Data Subjects require them for the establishment, exercise or defense of legal claims; or (iv) Data Subjects have objected to processing justified on any applicable legal basis, pending verification as to whether We have the legal basis to continue the processing;
g) object to the processing of the Data for the processing activities that are based on "consent";
h) request the erasure of the Data in prescribed circumstances according to applicable laws; and
i) obtain Data portability to receive the Data that had been previously supplied to Us in a structured, common use and readable format.

We may not always be able to grant your request. we will explain clearly whether we cannot accept your request, the rationale for our decision, and what will happen next.

13.2. **SWITZERLAND**

This Section 13.2 applies If the Swiss Federal Act on Data Protection ("**FADP**") applies to the Data processed relating to Data Subjects who are natural persons. When the Swiss Federal Act on Data Protection applies to the Data processed, the following provisions of the Privacy and Cookie Policy shall be read as follows:

13.2.1. Section 2: Please refer to Section 2 above for Reply's DPO contact details.

13.2.2. Section 9.3: If the FADP applies to Data transferred to recipients located in a country that does not have an adequate statutory level of data protection (as determined by the Swiss Federal Council), We will contractually require the recipient to comply with the FADP. For this purpose, We use standard contractual clauses approved by the Swiss Federal Data Protection and Information Commissioner (FDPIC). An exception may apply, for example, in the case of legal proceedings abroad, but also in cases of overriding public interest or if the performance of a contract requires disclosure, if Data Subjects have consented, or if Data Subjects have made the Data generally available and Data Subjects have not objected to the processing.

13.2.3. Section 11.1: This Section also applies if the processing of Data relating to Data Subject is subject to the FADP.

13.2.4. Section 11.4: Data Subjects located in Switzerland have the right to lodge a complaint with the competent data protection supervisory authority. You can reach the Swiss supervisory authority here: https://www.edoeb.admin.ch/edoeb/en/home/the-fdpic/contact.html.

13.3. **UNITED STATES**

ADDITIONAL INFORMATION FOR CALIFORNIA RESIDENTS

This subsection provides California residents with additional information regarding our collection, use and disclosure of their personal information, as well as their privacy rights, under the California Consumer Privacy Act (CCPA). This section does not address or apply to our handling of publicly available information or other personal information that is exempt under the CCPA.

Categories of Personal Information Collected and Disclosed. While our processing of personal information varies based upon our relationship and interactions with you, the table below identifies, generally, the categories of personal information (as defined by the CCPA) that we have collected about California residents, as well as the categories of third parties to whom we may disclose this information for a business or commercial purpose.

Categories of Personal Information Collected	Description	Categories of Third Parties to whom Personal Information is Disclosed
Identifiers	Includes direct identifiers, such as name, alias, user ID, and username; government identifiers such as Social Security Number (SSN) and driver's license number; email address, phone number, address and other contact information; IP address and other online identifiers; and other similar identifiers.	• affiliates and subsidiaries • business customer/client • business partners • advisors • government entities and law enforcement • others as required by law
Supplier Records	Includes personal information such as name, contact information, account number, and financial or payment information.	• affiliates and subsidiaries • business customer/client • business partners • advisors • government entities and law enforcement • others as required by law
Commercial Information	Includes records of products or services obtained, or considered, or use histories or tendencies.	• affiliates and subsidiaries • business customer/client • business partners • advisors • government entities and law enforcement • others as required by law
Internet or Electronic Network Activity Information	Includes browsing history, clickstream data, search history, access logs and other usage data and information regarding an individual's interaction with our Site, Services	• affiliates and subsidiaries • operating systems and platforms • business customer/client • business partners • advisors • government entities and law enforcement • others as required by law
Location Data	Location information about a particular individual or device (e.g., IP address).	• affiliates and subsidiaries • government entities and law enforcement • others as required by law

Audio, Video, and Electronic Data	Photographs and images (e.g., that you provide us)	• affiliates and subsidiaries • operating systems and platforms • business customer/client • business partners • advisors • government entities and law enforcement • others as required by law
Professional information	Includes professional and employment-related information (such as current and former employer(s) and position(s), business contact information, and professional memberships or licenses).	• affiliates and subsidiaries • business customer/client • business partners • advisors • government entities and law enforcement • others as required by law • client
Education Information	Includes information about education history or background that is not publicly available personally identifiable information as defined in the federal Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).	• affiliates and subsidiaries • business customer/client • business partners • advisors • government entities and law enforcement • others as required by law • client
Protected Classifications	Includes characteristics of protected classifications under California or federal law such as sex, age, citizenship status In section 4.6 of this Privacy and Cookie Policy, we have explicitly stated that we do not require any additional Protected or Classified information from the Data Subjects. However, if such information is provided to Us incidentally or voluntarily by the Data Subjects, we will not retain or process it further. Instead, it will be promptly deleted.	• affiliates and subsidiaries • business customer/client • business partners • advisors • government entities and law enforcement • others as required by law • customer/client
Sensitive Personal Information	Includes Social security, driver's license, state identification card, or passport number. The contents of an email, and text messages unless the business is the intended recipient of the communication.	• affiliates and subsidiaries • operating systems and platforms • business customer/client • business partners • advisors and agents • government entities and law enforcement • others as required by law

Sources of Personal Information. We generally collect Personal Information from the following categories of sources: directly and indirectly from you; affiliates and subsidiaries; customers.

Purposes of Collection, Use, and Disclosure. As described above in Section 5 (Data Processing Purposes and Legal Grounds for the Processing) and Section 7. Third Parties and Data Recipients, in general, we may collect, use, disclose, and otherwise process personal information for the following business or commercial purposes and as otherwise directed or consented to by you:

- Access and Maintenance Purposes;
- Pre-contractual Purposes;
- Contractual Purposes;
- Legal Obligation Purposes; and
- Legitimate Interest Purposes.

Sensitive Personal Information. We do not collect, use, or disclose "sensitive personal information" beyond the purposes authorized by the CCPA. Accordingly, we only use and disclose sensitive personal information as reasonably necessary and proportionate: (i) to perform our services; (ii) to help ensure security and integrity, including to prevent, detect, and investigate security incidents; (iii) to detect, prevent and respond to malicious, fraudulent, deceptive, or illegal conduct; (iv) to verify or maintain the quality and safety of our services; (v) for compliance with our legal obligations; (vi) to our third parties service providers who perform services on our behalf and (vii) for purposes other than inferring characteristics about you.

Sales and Sharing of Personal Information. The CCPA defines "sale" as disclosing or making available personal information to a third-party in exchange for monetary or other valuable consideration, and "sharing" includes disclosing or making available personal information to a third-party for purposes of cross-context behavioral advertising.

We neither disclose Personal Information to third parties in exchange for monetary compensation nor sell or share Personal Information, including sensitive personal information or information about individuals under sixteen years old.

Retention. We retain the personal information we collect only as reasonably necessary for the purposes described above or otherwise disclosed to you at the time of collection and as otherwise necessary to comply with our legal obligations, resolve disputes, maintain appropriate business records, and enforce our agreements. In some cases we may aggregate or de-identify information, such that it is no longer linked or reasonably linkable to you, and we may maintain such non-identifiable information indefinitely.

Privacy Rights for California Residents. The CCPA provides California residents with specific rights regarding personal information. Subject to certain conditions and exceptions, California residents have the following rights with respect to their personal information:

- ***Right to Know***. You have the right to request: (i) the categories or personal information we collected about you; (ii) the categories of sources from which the personal information is collected; (iii) our business or commercial purposes for collecting, selling, or sharing personal information; (iv) the categories of third parties to whom we have disclosed personal information; and (v) a copy of the specific pieces of personal information we have collected about you.
- ***Right to Delete***. You have the right to request we delete personal information we have collected from you.
- ***Right to Correct***. You have the right to request that we correct inaccuracies in your personal information.
- ***Right to Opt-Out of Sales and Sharing*.** You have the right to opt-out of "sales" and "sharing" of your personal information, as those terms are defined under the CCPA.

- ***Right to Limit Use and Disclosure***. You have the right to limit use and disclosure of your sensitive personal information. We do not use or disclose sensitive personal information beyond the purposes authorized by the CCPA; thus, this right is not available to California residents.
- ***Right to Non-Discrimination***. You have the right not to be subjected to discriminatory treatment for exercising any of the rights described in this section.

Submitting Privacy Requests. California residents may exercise their CCPA privacy rights as set forth below:

- ***Right to Know, Delete, Correct.*** California residents may submit verifiable requests to access/know, delete, and correct their personal information as well as request to limit the use and disclosure of their personal information by emailing us at supplier.privacy@reply.com.

  Verification. If you submit a request to access/know, correct, delete, or limit the use/disclosure of your personal information, we will take steps to verify your request by matching the information provided by you with the information we have in our records. We will process your request based upon the personal information in our records that is linked or reasonably linkable to the information provided in your request. In some cases, we may request additional information in order to verify your request or where necessary to process your request.

  Authorized Agent. You may also designate someone as an authorized agent to submit requests and act on your behalf. Authorized agents will be required to provide proof of their authorization in their first communication with us, and we may also require that the relevant consumer directly verify their identity and the authority of the authorized agent.
- ***Right to Opt-Out of Sales and Sharing***. To exercise your right to opt-out of the "sale" or "sharing" of your personal information, where applicable, you may do so following the instructions contained on the Site. We will apply your opt out based upon the personal information in our records that is linked or reasonably linkable to the information provided in your request.

Last update: september 2024