

HqO Privacy Policy

Introduction	3
(A) Data Privacy Framework Policy	4
1. Introduction	4
2. Scope of Certification	4
3. Independent Recourse Mechanism	6
4. Data Retention Policy	6
5. Security Measures	6
6. User Rights and Opt-Out Mechanisms	6
7. Enforcement and Dispute Resolution	7
8. Accountability for Onward Transfers Consistent with the DPF Principles	7
9. Security	8
10. Enforcement In compliance with the DPF Principles	8
11. Binding Arbitration (if necessary)	8
12. Regulatory Oversight	9
13. HqO Contact Information	9
14. Modifications & Updates	9
(B) HqO Privacy Policy for Site Visitors	10
1. Information We Collect	10
2. Data Retention Policy	11
3. Security Measures	11
4. User Rights and Opt-Out Mechanisms	11
5. Enforcement and Dispute Resolution	12
6. Our Use of Your Information and Legal Bases for Processing Information	12
7. Cookies and Online Advertising	13
a. Use of cookies	13
b. Opting out of Cookies	13
c. Online Advertising	14
8. Marketing	14
9. Our Disclosure of Your Information	15
10. Storing Your Information	15
11. Data Privacy Framework Principles	16
a. Data Privacy Framework (DPF) for EU-U.S. & UK-U.S. Transfers	16
b. Dispute Resolution & Complaints Handling	16
c. Compliance with PIPEDA	16
d. Compliance with APP 8.1	17
e. Standard Contractual Clauses (SCCs) for International Data Transfers (GDPR/EEA/UK)	17

12. Data Retention	17
13. Exclusions	18
14. Children	18
15. Links to Other Web Sites	18
16. Our Policy on Do Not Track Signals	19
17. Other Terms and Conditions	19
18. Changes to HqO's Privacy Policy	19
19. Your Rights	19
20. Privacy Rights	20
a. Your Privacy Rights for California Residents (CCPA/CPRA)	20
b. Rights for EU/EEA/UK Residents (GDPR & UK GDPR)	20
c. Rights for Canadian Residents (PIPEDA)	21
21. Federal Trade Commission (FTC)	21
22. Arbitration	21
23. Accountability for Onward Transfers Consistent with the DPF Principles	22
24. Contact Information	22
(C) HqO Privacy Policy for End-Users of HqO Services Offered by HqO Customers	23
1. Information We Collect	23
2. Data Retention Policy	24
3. Security Measures	25
4. User Rights and Opt-Out Mechanisms	25
5. Enforcement and Dispute Resolution	25
6. Our Use of Your Information and Legal Bases for Processing Information	25
7. Marketing	26
8. Our Disclosure of Your Information	27
9. Storing Your Information	28
10. Data Privacy Framework Principles	28
a. Data Privacy Framework (DPF) for EU-U.S. & UK-U.S. Transfers	28
b. Dispute Resolution & Complaints Handling	28
c. Compliance with Pipedata	29
d. Compliance with APP 8.1	29
e. Standard Contractual Clauses (SCCs) for International Data Transfers (GDPR/EEA/UK)	29
11. Data Retention	30
12. Exclusions	30
13. Children	30
14. Links to Other Web Sites	31
15. Security	31
16. Other Terms and Conditions	31
17. Changes to this Privacy Policy	31

18. Your Rights	32
19. Privacy Rights	32
a. Your Privacy Rights for California Residents (CCPA/CPRA)	32
b. Rights for EU/EEA/UK Residents (GDPR & UK GDPR)	33
c. Rights for Canadian Residents (PIPEDA)	33
16. Federal Trade Commission (FTC)	33
17. Arbitration	34
18. Accountability for Onward Transfers Consistent with the DPF Principles.	34
19. Contact Information	34
(D) HqO Privacy Policy for HqO Business Customers	35
1. Information We Collect	35
2. Data Retention Policy	36
3. Security Measures	36
4. User Rights and Opt-Out Mechanisms	36
5. Enforcement and Dispute Resolution	37
6. Our Use of Your Information and Legal Bases for Processing Information	37
7. Marketing	38
8. Our Disclosure of Your Information	38
9. Storing Your Information	39
10. Data Privacy Framework Principles	39
a. Data Privacy Framework (DPF) for EU-U.S. & UK-U.S. Transfers	39
b. Dispute Resolution & Complaints Handling	39
c. Compliance with Pipedata	40
d. Compliance with APP 8.1	40
e. Standard Contractual Clauses (SCCs) for International Data Transfers (GDPR/EEA/UK)	40
11. Data Retention	41
12. Exclusions	41
13. Security	41
14. Changes to HqO's Privacy Policy	42
15. Your Rights	42
16. Privacy Rights	43
a. Your Privacy Rights for California Residents (CCPA/CPRA)	43
b. Rights for EU/EEA/UK Residents (GDPR & UK GDPR)	43
c. Rights for Canadian Residents (PIPEDA)	43
13. Federal Trade Commission (FTC)	44
14. Arbitration	44
15. Accountability for Onward Transfers Consistent with the DPF Principles	44
16. Contact Information	45
Schedule I - Affiliates of HqO, Inc.	45

Introduction

DATE OF LAST REVISION: April 16th, 2025

Welcome to the Privacy Policy of HqO, Inc (“HqO”, “we”, “us” and/or “our”).

This Privacy Policy is provided by HqO and has been created to provide information about how we collect and process information through the HqO website (“the Site”), mobile applications (“App”), and services provided by us (the “HqO Services”), as well as from our business customers who use our business services (the “HqO Business Customer Services”). This Privacy Policy is divided into 3 parts depending on what type of user of the HqO services you are:

- A. Site visitors, who are individuals visiting our website to learn more about HqO, in which case the “HqO Privacy Policy for Site Visitors” applies to you;
- B. End-Users of HqO Services offered by HqO customers, in which case the “HqO Privacy Policy for End Users of HqO Services Offered by HqO Customers” applies to you; and
- C. HqO business customers, in which case the “HqO Privacy Policy for HqO Business Customers” applies to you

(A) Data Privacy Framework Policy

1. Introduction

HqO, Inc. complies with the requirements of the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), as set forth by the U.S. Department of Commerce.

HqO has certified to the U.S. Department of Commerce that it adheres to the DPF Principles with respect to personal information (as described below) that is transferred from the European Union and its Member States, the European Economic Area, the United Kingdom (and Gibraltar), and/or Switzerland to the United States.

If there is any conflict between the terms in this DPF Policy or another applicable privacy policy and the DPF Principles, the DPF Principles shall govern.

To learn more about the Data Privacy Framework and to view HqO's certification, please visit: <https://www.dataprivacyframework.gov>.

If there is any conflict between the terms in this Privacy Policy and the DPF Principles, the DPF Principles shall govern.

To learn more about the Data Privacy Framework and to view HqO's certification, please send a request to legal@hqo.co

2. Scope of Certification

HqO, Inc. is the sole U.S. entity certified under the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF. No U.S.-based affiliates or subsidiaries are included in HqO's DPF certification. References to "HqO and its affiliates" in this Privacy Policy pertain only to operational or organizational relationships and not to the scope of DPF certification.

This DPF Policy applies to personal information within the scope of HqO's DPF certification, which covers the following categories of information:

- Personal information regarding current, former and prospective partners, principals and employees for the purposes of operating and managing HqO, performing human resource administration and maintaining contact with individuals.
- Personal information regarding current, former and prospective clients and their personnel, customers, or other data subjects for the purposes of delivering HqO services, maintaining ongoing relationships and performing business development activities.

- Personal information regarding our suppliers, service providers, and other third parties, and their personnel for the purposes of managing and administering HqO's business relationships with such third parties.

3. Independent Recourse Mechanism

For unresolved complaints concerning personal data transferred under the DPF, HqO, Inc. has selected the EU Data Protection Authorities (DPAs), the UK Information Commissioner's Office (ICO), and the Swiss Federal Data Protection and Information Commissioner (FDPIC) as its designated Independent Recourse Mechanisms (IRMs), as applicable. HqO has fulfilled all related requirements, including payment of the annual fee to the United States Council for International Business (USCIB), which manages the DPA panel under U.S. Department of Commerce guidelines.

4. Data Retention Policy

HqO retains personal data only for as long as necessary to fulfill the purposes for which it was collected or as required by applicable law. Specifically:

- Client and customer data: Retained for up to five years post-contract expiration, unless legal retention is required.
- HR data: Retained for seven years after employment termination.
- Marketing and analytics data: Retained for two Years, unless the individual opts out sooner.

Once data is no longer needed, HqO securely deletes or anonymizes it.

5. Security Measures

HqO takes appropriate technical and organizational measures to protect personal data against loss, misuse, unauthorized access, disclosure, alteration, and destruction. Our security protocols include:

- Data encryption (AES-256 for stored data, TLS 1.2+ for transmitted data).
- Access control measures to restrict unauthorized personnel from accessing sensitive data.
- Incident response procedures for detecting, containing, and mitigating data breaches.

6. User Rights and Opt-Out Mechanisms

HqO respects individuals' rights under DPF and applicable data protection laws. Users may exercise the following rights:

- Right to access & correct Data: Users can request a copy of their data and request corrections if inaccurate.

- Right to delete data: Users can request deletion of their personal data where no legal retention is required.
- Right to limit use & Disclosure (opt-out). Users can opt-out of marketing communications via an unsubscribe link in emails or by contacting legal@hqo.co.

Requests can be submitted through our Privacy Request Form or via legal@hqo.co.

7. Enforcement and Dispute Resolution

HqO is committed to resolving complaints regarding our collection and use of personal data in compliance with the DPF Principles. Users may submit complaints to HqO directly via legal@hqo.co.

We aim to resolve any dispute you may raise within 45 days.

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, HqO, Inc. commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO), and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.

8. Accountability for Onward Transfers Consistent with the DPF Principles

HqO may transfer personal information to third parties, including transfers from one country to another. We will only disclose an individual's personal information to third parties under one or more of the following conditions:

- The disclosure is to a third party providing services to HqO, or to the individual, in connection with the operation of our business, and as consistent with the purpose for which the personal information was collected. We maintain written contracts with these third parties and require that these third parties provide at least the same level of privacy protection and security as required by the DPF Principles. To the extent provided by the DPF Principles, HqO remains responsible and liable under the DPF Principles if a third party that it engages to process personal information on its HqO | HqO's Data Privacy Framework Policy 2 behalf does so in a manner inconsistent with the DPF Principles, unless HqO proves that it is not responsible for the matter giving rise to the damage;
- With the individual's permission to make the disclosure;
- Where required to the extent necessary to meet a legal obligation to which HqO is subject, including a lawful request by public authorities and national security or law enforcement obligations and applicable law, rule, order, or regulation;
- Where reasonably necessary for compliance or regulatory purposes, or for the establishment of legal claims. Individual rights Individuals whose personal information is

covered by this DPF Policy have the right to access the personal information that HqO maintains about them as specified in the DPF Principles. Individuals may contact us to correct, amend or delete such personal information if it is inaccurate or has been processed in violation of the DPF Principles (except when the burden or expense of providing access, correction, amendment, or deletion would be disproportionate to the risks to the individual's privacy, or where the rights of persons other than the individual would be violated). Individuals may also have the right to limit the use and disclosure of their personal information (opt out) under certain circumstances, such as marketing. Requests to access, correct, amend, delete, or limit the use and disclosure of personal information (opt out) may be submitted using our request form.

9. Security

HqO takes appropriate measures to protect personal information in its possession to ensure a level of security appropriate to the risk of loss, misuse, unauthorized access, disclosure, alteration, and destruction. These measures take into account the nature of the personal information and the risks involved in its processing, as well as best practices in the industry for security and data protection.

10. Enforcement In compliance with the DPF Principles

HqO has a policy of responding to individuals within forty five days of an inquiry or complaint.

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, HqO, Inc. commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO), and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.

11. Binding Arbitration (if necessary)

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, HqO, Inc. commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF in

the context of the employment relationship. This applies to parts A, B, and C of the Privacy Policy.

If the dispute remains unresolved after ADR, individuals may invoke binding arbitration under the DPF Panel's rules, provided they have completed all prior resolution steps.

12. Regulatory Oversight

HqO is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC).

13. HqO Contact Information

No matter what type of user you are, you have any questions about HqO's Privacy Policy or the information practices of the HqO Services, or wish to exercise any of your data protection rights as described in the sections below, please email legal@hqo.co.

14. Modifications & Updates

HqO may update this policy periodically to reflect regulatory changes or operational adjustments. Any material changes will be communicated via our website or direct user notifications.

If you are a resident of the United Kingdom or European Economic Area, please note that we have appointed an EU data protection representative. For further inquiries, please contact our Data Protection Officer (DPO) at: legal@hqo.co.

(B) HqO Privacy Policy for Site Visitors

HqO, Inc., is the Controller of your information collection through your use of our Site pursuant to the EU General Data Protection Regulation 2016/679, as applicable.

As a Data Controller, we determine the purposes and means of processing this personal data in accordance with GDPR, UK GDPR, and applicable data protection laws.

Please read this section of Privacy Policy to understand how we may process your information via your use of our Site. If you do not agree with how we process your information, please do not use the Site.

1. Information We Collect

When you interact with us through the Site, we may collect your information from and about you, as further described below:

- **Information That You Provide:** We collect information from you when you voluntarily provide it, such as when you contact us with inquiries, respond to one of our surveys, or provide it at conference or event. This information may include your name, business contact information, and title.
- **Interaction with our Site:** When you interact with HqO through the Site, we receive and store certain information automatically through various technologies. HqO may store such information itself or such information may be included in databases owned and maintained by HqO affiliates, agents or service providers. This Site may use such information and pool it with other information to track, for example, the total number of visitors to our Site, the number of visitors to each page of our Site, and the domain names of our visitors' Internet service providers. For further details please see the section on "Cookies" below.
- **Research and Analytics Data:** In an ongoing effort to better understand and serve the users of the HqO Services, HqO often conducts research on its Site visitor demographics, interests and behavior based on the information you provide to us and that we collect from and about you. This research may be compiled and analyzed on an aggregate and/or de-identified basis, in which case HqO may share this aggregated and/or de-identified data with its affiliates, agents and business partners. This aggregate and/or de-identified information cannot be used to identify you personally. HqO may also disclose aggregated user statistics to describe our services to current and prospective business partners, and to other third parties for other lawful purposes.

2. Data Retention Policy

HqO retains personal data only for as long as necessary to fulfill the purposes for which it was collected or as required by applicable law. Specifically:

- Client and customer data: Retained for up to five years post-contract expiration, unless legal retention is required.
- HR data: Retained for seven years after employment termination.
- Marketing and analytics data: Retained for two Years, unless the individual opts out sooner.

Once data is no longer needed, HqO securely deletes or anonymizes it.

3. Security Measures

HqO takes appropriate technical and organizational measures to protect personal data against loss, misuse, unauthorized access, disclosure, alteration, and destruction. Our security protocols include:

- Data encryption (AES-256 for stored data, TLS 1.2+ for transmitted data).
- Access control measures to restrict unauthorized personnel from accessing sensitive data.
- Incident response procedures for detecting, containing, and mitigating data breaches.

4. User Rights and Opt-Out Mechanisms

HqO respects individuals' rights under DPF and applicable data protection laws. Users may exercise the following rights:

- Right to access & correct Data: Users can request a copy of their data and request corrections if inaccurate.
- Right to delete data: Users can request deletion of their personal data where no legal retention is required.
- Right to limit use & Disclosure (opt-out). Users can opt-out of marketing communications via an unsubscribe link in emails or by contacting legal@hgo.co.

Requests can be submitted through our Privacy Request Form or via legal@hgo.co.

5. Enforcement and Dispute Resolution

HqO is committed to resolving complaints regarding our collection and use of personal data in compliance with the DPF Principles. Users may submit complaints to HqO directly via legal@hqo.co

We aim to resolve any dispute you may raise within 45 days.

6. Our Use of Your Information and Legal Bases for Processing Information

We process information you provide to us to enable us to provide the Site to you pursuant to any applicable Site terms, to ensure compliance with local legal and regulatory requirements, and for the purposes of our legitimate business interests, including to:

- enable us to provide you with the information, products and services that you request from us;
- enable us to respond to an inquiry or other request you make when you contact us via our Site, including for customer services support;
- notify you about any changes to the Site;
- enable us to issue a notice or corrective action to you in relation to the Site, if required;
- help us improve the content and functionality of the Site and HqO Services, and to better understand and analyze how you use our Site;
- detect security incidents, and protect against malicious, deceptive, fraudulent, or illegal activity;
- troubleshoot and debug Site;
- provide you with information about other services which we believe will be of interest to you similar to those that you have already purchased or inquired about, as described in the “Marketing” section below.

We process personal information under the following legal bases, depending on the applicable jurisdiction:

- GDPR / UK GDPR: We rely on legitimate interest, contract performance, legal obligation, and consent, as required, to process personal data.
- CCPA: We process data for business purposes, consumer consent, and service provision, in compliance with California privacy laws.
- PIPEDA: We rely on implied or express consent, except where legal exceptions apply.
- Australia (APPs): We collect personal information directly where necessary for our business operations, relying on individual consent where required under the Australian Privacy Act.

7. Cookies and Online Advertising

a. Use of cookies

In operating our Site, we may use a technology called “cookies”. A cookie is a piece of information that the computer that hosts our Site stores to your browser when you access the Site. We use:

- Various types of cookies, including session cookies, persistent cookies, local shared objects, pixels, gifs and other tracking technologies, session and persistent technologies, first and third-party cookies. Cookies can be persistent by remaining on your computer until you delete them or be based on your browsing session where they delete once you close your browser. First party cookies are used and controlled by us to provide services on our Site. Our use of cookies falls into three categories:
- Strictly necessary cookies: these are essential to enable you to move around our Site and use its features. Without these cookies, the services you have asked for cannot be provided.
- Performance cookies: also known as “analytical” cookies. These cookies allow us to recognize and count the number of visitors and to see how visitors move around our site. For example, they allow us to understand which pages are visited most often, and if they get error messages from web pages. All information collected by these cookies is aggregated and therefore anonymous.
- Advertising cookies: Through the help of third-party service providers, we may place certain cookies on our Site that allow us to provide advertising for the HqO Services both on and off the Site, as explained below.

Strictly necessary cookies are necessary to provide the Site to you. We use such cookies without your prior consent. All other cookies are dropped after you have consented via a cookie banner.

b. Opting out of Cookies

You have the ability to accept or decline cookies. Most browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. Detailed instructions are provided by your browser. If you do not accept all cookies or withdraw your consent, you may still browse the Site; however, in this case you may not be able to use the full functionalities of the Site. For more information on cookies and how they can be managed and deleted please visit <https://www> or your browser cookie settings.

c. Online Advertising

We and non-affiliated third parties performing services on our behalf may integrate advertising technologies that allow for the delivery of relevant advertising on the Site, as well as on other websites you visit. The ads may be based on various factors such as the content of the page you are visiting, demographic data, and other information we and our service providers collect from or about you. These ads may be based on your current activity or your activity over time and across other websites and online services and may be tailored to your interests.

We neither have access to, nor does this Privacy Policy govern, the use of cookies or other tracking technologies that may be placed on your device you use to access the Services by such non-affiliated third parties. If you are interested in more information about tailored browser advertising and how you can generally control cookies from being put on your computer to deliver tailored advertising, you may visit the Network Advertising Initiative's Consumer Opt-Out Link, the Digital Advertising Alliance's Consumer Opt-Out Link, or Your Online Choices to opt-out of receiving tailored advertising from companies that participate in those programs. To opt out of Google Analytics for display advertising or customize Google display network ads, visit the Google Ads Settings page. We do not control these opt-out links or whether any particular company chooses to participate in these

opt-out programs. We are not responsible for any choices you make using these mechanisms or the continued availability or accuracy of these mechanisms.

Please note that if you exercise the opt out choices above, you will still see advertising when you use the Site, but it will not be tailored to you based on your online behavior over time.

8. Marketing

HqO and its Affiliates (see Schedule I for list of affiliates) (the "HqO Related Companies") may also use your information to contact you via email, phone, or postal mail with promotional materials in the future to tell you about services we believe will be of interest to you, in accordance with applicable law.

Note: References to 'HqO and its affiliates' refer to operational business relationships. Only HqO, Inc. is certified under the DPF.

In our promotional emails, there will be instructions explaining how to "opt-out" of receiving them in the future, if you would like. In addition, if at any time you wish not to receive any future promotional communications or you wish to have your name deleted from our mailing lists, please contact us as indicated below. Please note that it may take time to process your request,

consistent with our legal obligations. Also, after you have opted out, you may continue to receive non-promotional, transactional communications from us.

9. Our Disclosure of Your Information

We may share your information with certain third parties, as set forth below:

- **Business Transfers:** As we develop our business, we might sell or buy some or all of our businesses or assets. In the event of a corporate sale, merger, reorganization, dissolution or similar event, your information may be part of the transferred assets.
- **Related Companies:** We may also share information with our HqO Related Companies for purposes consistent with this Privacy Policy.
- **Agents, Consultants and Related Third Parties:** HqO, like many businesses, sometimes hires other companies to perform certain business-related functions on our behalf. Examples of such functions include hosting our HqO Services, mailing information, sales and marketing, shipping and fulfillment, maintaining databases, and processing payments. When we employ another company to perform a function of this nature, we only provide them with the information that they need to perform their specific function.
- **Legal Requirements:** HqO may disclose your information if required to do so by law or in the good faith belief that such action is necessary to (i) comply with a legal obligation, (ii) protect and defend the rights or property of HqO, (iii) act in urgent circumstances to protect the personal safety of users of the Site or the public, or (iv) protect against legal liability.

When we disclose your personal data to third parties, we take reasonable measures to ensure that the rules set out in this Privacy Policy are complied with and that these third parties provide sufficient guarantees to implement appropriate technical and organizational measures to protect your personal data.

10. Storing Your Information

Your information collected via our Site will be stored on servers located in the United States, European Union and other locations that may have different data protection laws than in your jurisdiction. This includes by individuals or service providers engaged in, among other things, administration of an enquiry or request you make via our Site, or the provision of support services. By using the Site, you acknowledge that your information will be stored and processed in the United States, European Union and potentially other global locations.

11. Data Privacy Framework Principles

a. Data Privacy Framework (DPF) for EU-U.S. & UK-U.S. Transfers

HqO complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. These frameworks govern the processing of Personal Data (as defined by applicable EU, UK, and Swiss data protection laws) transferred to the United States from these regions.

HqO has certified to the U.S. Department of Commerce that it adheres to the DPF Principles with respect to the processing of personal data received under these frameworks. If any conflict arises between the terms in this privacy policy and the DPF Principles, the DPF Principles shall govern.

To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>.

b. Dispute Resolution & Complaints Handling

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, HqO, Inc. commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO), and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.

On 4 June 2021, the Commission issued modernised standard contractual clauses under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR).

These modernised SCCs replace the three sets of SCCs that were adopted under the previous Data Protection Directive 95/46. Consequently, we are relying on standard contractual clauses (based on the clauses published [here](#), a copy of which can be obtained by contacting us at legal@hqo.co) for transfers of personal data from the EEA.

c. Compliance with PIPEDA

HqO complies with the Personal Information Protection and Electronic Documents Act (PIPEDA) and its contractual obligations for international transfers.

HqO implements contractual safeguards in accordance with PIPEDA, including binding contractual clauses with our service providers.

We conduct periodic assessments to verify that our international data recipients comply with these contractual obligations and maintain adequate data protection measures.

Canadian users who have concerns about international data transfers may contact us at legal@hqo.co for more details.

d. Compliance with APP 8.1

HqO complies with the Australian Privacy Act 1988 and the Australian Privacy Principles (APPs).

HqO meets Australian legal requirements by:

- Implementing contractual safeguards with overseas recipients.
- Conducting risk assessments to evaluate whether the recipient provides an adequate level of data protection.
- Obtaining consent where necessary before transferring sensitive personal data internationally.
- If you are an Australian resident and have concerns about how your personal data is handled under APP 8.1, you can contact us at legal@hqo.co

e. Standard Contractual Clauses (SCCs) for International Data Transfers (GDPR/EEA/UK)

On 4 June 2021, the European Commission issued modernized Standard Contractual Clauses (SCCs) under the GDPR for data transfers from controllers or processors in the EU/EEA/UK to non-EU/EEA/UK recipients.

These modernized SCCs replace previous SCCs that were based on the Data Protection Directive 95/46.

HqO relies on SCCs as an approved mechanism for transferring personal data from the EEA/UK to third countries (including the U.S.).

A copy of the Standard Contractual Clauses (SCCs) used by HqO is available upon request via legal@hqo.co

12. Data Retention

We will only retain your information for as long as necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for your information, we consider the amount, nature, and sensitivity of the information, the potential risk of harm from unauthorized use or disclosure of your information, the purposes for which we process your information and whether we can achieve those purposes through other means, and the applicable legal requirements.

13. Exclusions

This HqO Privacy Policy for Site Visitors does not apply to information collected by HqO other than information collected through the Site. This Privacy Policy will not apply to any unsolicited information you provide to HqO through this Site or through any other means. This includes, but is not limited to, information posted to any public areas of the Site, such as bulletin boards (collectively, “Public Areas”), any ideas for new products or modifications to existing products, and other unsolicited submissions (collectively, “Unsolicited Information”). All Unsolicited Information will be deemed to be non-confidential and HqO will be free to reproduce, use, disclose, and distribute such Unsolicited Information to others without limitation or attribution.

14. Children

The Site is intended for general audiences and not for children under the age of 13. If we become aware that we have collected “personal information” (as defined by the United States Children’s Online Privacy Protection Act) from children under the age of 13 without legally valid parental consent, we will take reasonable steps to delete it as soon as possible. We do not knowingly process data of EU residents under the age of 16 without parental consent. If we become aware that we have collected data from an EU resident under the age of 16 without parental consent, we will take reasonable steps to delete it as soon as possible. We also comply with other age restrictions and requirements in accordance with applicable local laws.

15. Links to Other Web Sites

This Site may contain links to other web sites not operated or controlled by HqO (the “Third Party Sites”). The policies and procedures we described here do not apply to such Third Party Sites. The links from this Site do not imply that HqO endorses or has reviewed the Third Party Sites. We suggest contacting those sites directly for information on their privacy policies and practices.

16. Our Policy on Do Not Track Signals

This Site may contain links to other web sites not operated or controlled by HqO (the “Third Party Sites”). The policies and procedures we described here do not apply to such Third Party Sites. The links from this Site do not imply that HqO endorses or has reviewed the Third Party Sites. We suggest contacting those sites directly for information on their privacy policies and practices. HqO takes steps to protect the information provided via the Site from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. However, no Internet or e-mail transmission is ever fully secure or error free. Please keep this in mind when disclosing any information to HqO.

17. Other Terms and Conditions

Your access to and use of this Site is subject to the Terms of Use.

18. Changes to HqO's Privacy Policy

The Site, our business, and applicable legal requirements may change from time to time. As a result, at times it may be necessary for HqO to make changes to this Privacy Policy. HqO reserves the right to update or modify this Privacy Policy at any time in accordance with our legal obligations. Please review this policy periodically. This Privacy Policy was last updated on the date indicated above. Your continued use of the Site after any changes or revisions to this Privacy Policy will indicate your agreement with the terms of such revised Privacy Policy.

19. Your Rights

To keep your information accurate, current, and complete, please contact us as specified at the beginning of this Privacy Policy. We will take reasonable steps to update or correct your information in our possession in accordance with applicable law.

You may have the right to: request access to your Personal Data we hold about you; request we correct any inaccurate Personal Data we hold about you; request we delete any Personal Data we hold about you; restrict the processing of Personal Data we hold about you; object to the processing of Personal Data we hold about you; and/or receive any Personal Data we hold about you in a structured and commonly used machine-readable format or have such Personal Data transmitted to another company. We may ask you for additional information to confirm your identity and for security purposes, before disclosing information requested to you. We will process any request in line with any local laws and our policies and procedures. If you are located in the EEA or United Kingdom, you have the right to lodge a complaint about how we process your Personal Data with the supervisory authority in your country.

If you wish to exercise any of your rights, please contact us using the information provided in the section.

20. Privacy Rights

a. Your Privacy Rights for California Residents (CCPA/CPRA)

Under the CCPA and CPRA, California residents have the following rights:

- Right to Request and Receive Personal Information Disclosures
- Right to Delete Personal Information
- Right to Correct Inaccurate Personal Information
- Right to Know What Personal Information is Being Collected and Access Personal Information
- Right to Know What Personal Information is Sold or Shared, and to Whom
- Right to Opt-Out of the Sale or Sharing of Personal Information
- Right to Limit Use and Disclosure of Sensitive Personal Information
- Right of Non-Retaliation

If you are a California resident and wish to exercise any of these rights, please contact us using the information provided in our Privacy Notice.

b. Rights for EU/EEA/UK Residents (GDPR & UK GDPR)

Under the General Data Protection Regulation (GDPR) and UK GDPR, individuals in the European Economic Area (EEA), United Kingdom (UK), and Switzerland have the following rights:

- Right to Access
- Right to Rectification
- Right to Erasure ("Right to be Forgotten")
- Right to Restriction of Processing
- Right to Data Portability
- Right to Object
- Right to Withdraw Consent
- Right to Lodge a Complaint

To exercise your GDPR rights or inquire about how we process your data, please contact us through the details provided in our Privacy Notice.

c. Rights for Canadian Residents (PIPEDA)

If you are a resident of Canada, your personal information is protected under the Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial privacy laws. Your rights under PIPEDA include:

- Right to Access
- Right to Correction
- Right to Withdraw Consent
- Right to Challenge Compliance

Under PIPEDA, we process personal information based on:

- Implied or Express Consent – We may rely on either express consent (e.g., signing a form) or implied consent (where the purpose is obvious).
- Legal Exceptions – In some cases, we may process personal data without consent, such as for fraud prevention, legal compliance, or investigations.

21. Federal Trade Commission (FTC)

HqO is subject to the investigatory and enforcement powers of the FTC.

22. Arbitration

HqO is obligated to arbitrate claims and follow the terms as set forth in Annex I of the DPF Principles, provided that an individual has invoked binding arbitration by delivering notice to HqO and following the procedures and subject to conditions set forth in Annex I of Principles.

If the dispute remains unresolved after ADR, individuals may invoke binding arbitration under the DPF Panel's rules, provided they have completed all prior resolution steps.

23. Accountability for Onward Transfers Consistent with the DPF Principles

HqO may transfer personal information to third parties, including transfers from one country to another. We will only disclose an individual's personal information to third parties under one or more of the following conditions:

- The disclosure is to a third party providing services to HqO, or to the individual, in connection with the operation of our business, and as consistent with the purpose for which the personal information was collected. We maintain written contracts with these third parties and require that these third parties provide at least the same level of privacy protection and security as required by the DPF Principles. To the extent provided by the DPF Principles, HqO remains responsible and liable under the DPF Principles if a third party that it engages to process personal information on its behalf does so in a manner inconsistent with the DPF Principles, unless HqO proves that it is not responsible for the matter giving rise to the damage;
- With the individual's permission to make the disclosure;
- Where required to the extent necessary to meet a legal obligation to which HqO is subject, including a lawful request by public authorities and national security or law enforcement obligations and applicable law, rule, order, or regulation;
- Where reasonably necessary for compliance or regulatory purposes, or for the establishment of legal claims.

24. Contact Information

HqO may update this policy periodically to reflect regulatory changes or operational adjustments. Any material changes will be communicated via our website or direct user notifications.

If you are a resident of the United Kingdom or European Economic Area, please note that we have appointed an EU data protection representative. For further inquiries, please contact our Data Protection Officer (DPO) at: legal@hqo.co.

(C) HqO Privacy Policy for End-Users of HqO Services Offered by HqO Customers

To the extent that you are providing information via the mobile applications (“App”) in connection with your occupation or use of a building or particular physical space (“End-Users”) in which you live, visit or work, please note that HqO processes this information on behalf of our customers who are building or space owners (“Customer Data”) to provide HqO services, including access to the HqO Platform and Tenant Experience applications (the “HqO Services”) to you as an App End User. We are a processor when we process Customer Data, our customer is the data controller. This Privacy Policy explains the information collected from and about you as an End User of the App.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, HqO, Inc. commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner’s Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF in the context of the employment relationship. This applies to parts A, B, and C of the Privacy Policy.

Please read this Privacy Policy to understand how we and our Customers (together referred to herein as “we”) may process your information via your use of the HqO Services. If you do not agree with how we process your information, please do not use the HqO Services.

1. Information We Collect

When you interact with us through our Site, we may collect information from and about you, as further described below:

Information That You Provide: We collect information from you when you voluntarily provide it, such as when you contact us with inquiries, respond to one of our surveys, provide it at a conference or event, register for access to the HqO Services, or use certain HqO Services. This information may include your name, business contact information, and title.

Location Data: Some features and functionality in our HqO Services require that you provide your location. If you have location services turned on, whenever you use such HqO Services on your mobile device, we collect and use your geocoordinates (e.g. latitude and longitude) to tailor

the HqO Services to your current location. We will only process your location with your express permission. If you have persistent background location turned on, we will obtain your device's location even if you are not using the HqO Services on your mobile device. Your location is never shared with others, except with your consent or as permitted under this Privacy Policy. We use various technologies to determine your precise location, such as the location services of your operating system or browser, sensor data from your device (e.g. magnetometer, barometer, gyroscopes, accelerometers, compasses, Bluetooth data, beacon data, Wi-Fi access points, GPS data, and cell tower data), and other data that may help us understand your precise location. If you have opted-in to sharing your background location with us as part of using the HqO Services, you may remove this permission at any time by going into your operating device settings and toggling off background sharing.

Interaction with our App: When you interact with the HqO Services through the App, we receive and store certain information automatically about your interaction with the App. We may store such information ourselves, or such information may be included in databases owned and maintained by our affiliates, agents or service providers. The HqO Services may use such information and pool it with other information to track, for example, the total number of App users, the number of users of different portions of the App, and similar App usage information.

Setting up an account via the App: when you download our App and set up an account, we will collect certain information from you such as your username and password in order to process your registration and administer your account.

Research and Analytics Data: In an ongoing effort to better understand and serve the users of the HqO Services, HqO often conducts research on its customer and user demographics, interests and behavior based on the information you provide to us. This research may be compiled and analyzed on an aggregate and/or de-identified basis, in which case HqO may share this aggregated and/or de-identified data with its affiliates, agents and business partners. This aggregate and/or de-identified information cannot be used to identify you personally. HqO may also disclose aggregated user statistics to describe our services to current and prospective business partners, and to other third parties for other lawful purposes.

2. Data Retention Policy

HqO retains personal data only for as long as necessary to fulfill the purposes for which it was collected or as required by applicable law. Specifically:

- Client and customer data: Retained for up to five years post-contract expiration, unless legal retention is required.
- HR data: Retained for seven years after employment termination.
- Marketing and analytics data: Retained for two Years, unless the individual opts out sooner.

Once data is no longer needed, HqO securely deletes or anonymizes it.

3. Security Measures

HqO takes appropriate technical and organizational measures to protect personal data against loss, misuse, unauthorized access, disclosure, alteration, and destruction. Our security protocols include:

- Data encryption (AES-256 for stored data, TLS 1.2+ for transmitted data).
- Access control measures to restrict unauthorized personnel from accessing sensitive data.
- Incident response procedures for detecting, containing, and mitigating data breaches.

4. User Rights and Opt-Out Mechanisms

HqO respects individuals' rights under DPF and applicable data protection laws. Users may exercise the following rights:

- Right to access & correct Data: Users can request a copy of their data and request corrections if inaccurate.
- Right to delete data: Users can request deletion of their personal data where no legal retention is required.
- Right to limit use & Disclosure (opt-out). Users can opt-out of marketing communications via an unsubscribe link in emails or by contacting legal@hgo.co.

Requests can be submitted through our Privacy Request Form or via legal@hgo.co.

5. Enforcement and Dispute Resolution

HqO is committed to resolving complaints regarding our collection and use of personal data in compliance with the DPF Principles. Users may submit complaints to HqO directly via legal@hgo.co.

We aim to resolve any dispute you may raise within 45 days.

6. Our Use of Your Information and Legal Bases for Processing Information

We process the information you provide to us to enable us to perform the contract we are about to enter into or have entered into with your landlord or your employers landlord, to ensure compliance with local legal and regulatory requirements, and for the purposes of our legitimate business interests, including to:

- to provide you with access to our Platform and the Services, to support your use of HqO Services, and to support the use of the HqO Services by others who interact with you through our HqO Services (such as your landlord, your property manager, your employer, or third party service providers)
- enable us to carry out our obligations arising from any contracts and to provide you with the information, products and services that you request from us;
- enable us to respond to an inquiry or other request you make when you contact us via our App, including for customer services support;
- notify you about any changes to the HqO Services;
- enable us to issue a notice or corrective action to you in relation to any of the HqO Services, if required;
- help us improve the content and functionality of the HqO Services, and to better understand and analyze how you use our App;
- detect security incidents, and protect against malicious, deceptive, fraudulent, or illegal activity;
- troubleshoot and debug HqO Services errors;
- provide you with information about other services which we believe will be of interest to you similar to those that you have already purchased or inquired about, as described in the “Marketing” section below.

We process personal information under the following legal bases, depending on the applicable jurisdiction:

- GDPR / UK GDPR: We rely on legitimate interest, contract performance, legal obligation, and consent, as required, to process personal data.
- CCPA: We process data for business purposes, consumer consent, and service provision, in compliance with California privacy laws.
- PIPEDA: We rely on implied or express consent, except where legal exceptions apply.
- Australia (APPs): We collect personal information directly where necessary for our business operations, relying on individual consent where required under the Australian Privacy Act.

7. Marketing

HqO and its affiliates (see Schedule I for list of affiliates) (the “HqO Related Companies”) may also use your information to contact you via email, phone, or postal mail with promotional materials in the future to tell you about services we believe will be of interest to you in accordance with applicable law.

Note: References to 'HqO and its affiliates' refer to operational business relationships. Only HqO, Inc. is certified under the DPF.

In our promotional emails, there will be instructions explaining how to “opt-out” of receiving them in the future, if you would like. In addition, if at any time you wish not to receive any future promotional communications or you wish to have your name deleted from our mailing lists, please contact us as indicated below. Please note that it may take time to process your request, consistent with our legal obligations. Also, after you have opted out, you may continue to receive non-promotional, transactional communications from us.

8. Our Disclosure of Your Information

We may share your information with certain third parties, as set forth below:

- **Business Transfers:** As we develop our business, we might sell or buy some or all of our businesses or assets. In the event of a corporate sale, merger, reorganization, dissolution or similar event, your information may be part of the transferred assets.
- **Related Companies:** We may also share your information with our HqO Related Companies for purposes consistent with this Privacy Policy.
- **Agents, Consultants and Related Third Parties:** We, like many businesses, sometimes hire other companies to perform certain business-related functions on our behalf. Examples of such functions include hosting the HqO Services, mailing information, sales and marketing, shipping and fulfillment, maintaining databases, and processing payments. When we employ another company to perform a function of this nature, we only provide them with the information that they need to perform their specific function.
- **Legal Requirements:** We may disclose your information if required to do so by law or in the good faith belief that such action is necessary to (i) comply with a legal obligation, (ii) protect and defend our rights or property, (iii) act in urgent circumstances to protect the personal safety of users of the HqO Services or the public, or (iv) protect against legal liability.

When we disclose your personal data to third parties, we take reasonable measures to ensure that the rules set out in this Privacy Policy are complied with and that these third parties provide sufficient guarantees to implement appropriate technical and organizational measures to protect your personal data.

9. Storing Your Information

Your information collected via the HqO Services will be stored on servers located in the United States, European Union and other locations that may have different data protection laws than in your jurisdiction. This includes individuals or service providers engaged in, among other things, and provision of support services. By using the HqO Services, you acknowledge that your information will be stored and processed in the United States, European Union and potentially other global locations.

10. Data Privacy Framework Principles

a. Data Privacy Framework (DPF) for EU-U.S. & UK-U.S. Transfers

HqO complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. These frameworks govern the processing of Personal Data (as defined by applicable EU, UK, and Swiss data protection laws) transferred to the United States from these regions.

HqO has certified to the U.S. Department of Commerce that it adheres to the DPF Principles with respect to the processing of personal data received under these frameworks. If any conflict arises between the terms in this privacy policy and the DPF Principles, the DPF Principles shall govern.

To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>.

b. Dispute Resolution & Complaints Handling

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, HqO, Inc. commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO), and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.

On 4 June 2021, the Commission issued modernised standard contractual clauses under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR).

These modernised SCCs replace the three sets of SCCs that were adopted under the previous

Data Protection Directive 95/46. Consequently, we are relying on standard contractual clauses (based on the clauses published [here](#), a copy of which can be obtained by contacting us at legal@hgo.co) for transfers of personal data from the EEA.

c. Compliance with Pippeda

HqO complies with the Personal Information Protection and Electronic Documents Act (PIPEDA) and its contractual obligations for international transfers.

HqO implements contractual safeguards in accordance with PIPEDA, including binding contractual clauses with our service providers.

We conduct periodic assessments to verify that our international data recipients comply with these contractual obligations and maintain adequate data protection measures.

Canadian users who have concerns about international data transfers may contact us at legal@hgo.co for more details.

d. Compliance with APP 8.1

HqO complies with the Australian Privacy Act 1988 and the Australian Privacy Principles (APPs).

HqO meets Australian legal requirements by:

- Implementing contractual safeguards with overseas recipients.
- Conducting risk assessments to evaluate whether the recipient provides an adequate level of data protection.
- Obtaining consent where necessary before transferring sensitive personal data internationally.
- If you are an Australian resident and have concerns about how your personal data is handled under APP 8.1, you can contact us at legal@hgo.co.

e. Standard Contractual Clauses (SCCs) for International Data Transfers (GDPR/EEA/UK)

On 4 June 2021, the European Commission issued modernized Standard Contractual Clauses (SCCs) under the GDPR for data transfers from controllers or processors in the EU/EEA/UK to non-EU/EEA/UK recipients.

These modernized SCCs replace previous SCCs that were based on the Data Protection Directive 95/46.

HqO relies on SCCs as an approved mechanism for transferring personal data from the EEA/UK to third countries (including the U.S.).

A copy of the Standard Contractual Clauses (SCCs) used by HqO is available upon request via legal@hqo.co.

11. Data Retention

We will only retain your information for as long as necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for your information, we consider the amount, nature, and sensitivity of the information, the potential risk of harm from unauthorized use or disclosure of your information, the purposes for which we process your information and whether we can achieve those purposes through other means, and the applicable legal requirements.

12. Exclusions

This Privacy Policy does not apply to information collected by us other than information collected through the HqO Services. This Privacy Policy will not apply to any unsolicited information you provide to HqO through any means. This includes, but is not limited to, any ideas for new products or modifications to existing products, and other unsolicited submissions (collectively, “Unsolicited Information”). All Unsolicited Information will be deemed to be non-confidential and we will be free to reproduce, use, disclose, and distribute such Unsolicited Information to others without limitation and attribution.

This Privacy Policy does not address, and we are not responsible for, the privacy, information, or other practices of any third parties with whom you interact using our HqO Services, including any landlord, property manager, tenant, merchant or service provider, and including any other third party operating any site, application or service that may be introduced, included or integrated into our HqO Services. We encourage you to read the privacy policy of every person with whom you interact using our HqO Services.

13. Children

HqO Services are intended for general audiences and not for children under the age of 13. If we become aware that we have collected “personal information” (as defined by the United States Children’s Online Privacy Protection Act) from children under the age of 13 without legally valid parental consent, we will take reasonable steps to delete it as soon as possible. We do not

knowingly process data of EU residents under the age of 16 without parental consent. If we become aware that we have collected data from an EU resident under the age of 16 without parental consent, we will take reasonable steps to delete as soon as possible. We also comply with other age restrictions and requirements in accordance with applicable local laws.

14. Links to Other Web Sites

This Privacy Policy applies only to the HqO Services. The HqO Services and App may contain links to other web sites not operated or controlled by HqO (the “Third Party Sites”). The policies and procedures we described here do not apply to such Third Party Sites. The links from the HqO Services do not imply that HqO endorses or has reviewed the Third Party Sites. We suggest contacting those sites directly for information on their privacy policies and practices.

15. Security

We take steps to protect the information provided via the HqO Services from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. However, no Internet or e-mail transmission is ever fully secure or error free. Please keep this in mind when disclosing any information to us.

16. Other Terms and Conditions

Your access to and use of the HqO Services is subject to the Terms of Use () and the End User License Agreement.

17. Changes to this Privacy Policy

Our business, and applicable legal requirements may change from time to time. As a result, at times it may be necessary for us to make changes to this Privacy Policy. We reserve the right to update or modify this Privacy Policy at any time in accordance with our legal obligations. Please review this policy periodically. This Privacy Policy was last updated on the date indicated above. Your continued use of the HqO Services after any changes or revisions to this Privacy Policy will indicate your agreement with the terms of such revised Privacy Policy.

18. Your Rights

To keep your information accurate, current, and complete, please contact us as specified below. We will take reasonable steps to update or correct your information in our possession in accordance with applicable law.

You may have the right to: request access to your Personal Data we hold about you; request we correct any inaccurate Personal Data we hold about you; request we delete any Personal Data we hold about you; restrict the processing of Personal Data we hold about you; object to the processing of Personal Data we hold about you; and/or receive any Personal Data we hold about you in a structured and commonly used machine-readable format or have such Personal Data transmitted to another company. We may ask you for additional information to confirm your identity and for security purposes, before disclosing information requested to you. We will process any request in line with any local laws and our policies and procedures. If you are located in the EEA or United Kingdom, you have the right to lodge a complaint about how we process your Personal Data with the supervisory authority in your country.

If you wish to exercise any of your rights, please contact us using the information provided in the section.

19. Privacy Rights

a. Your Privacy Rights for California Residents (CCPA/CPRA)

Under the CCPA and CPRA, California residents have the following rights:

- Right to Request and Receive Personal Information Disclosures
- Right to Delete Personal Information
- Right to Correct Inaccurate Personal Information
- Right to Know What Personal Information is Being Collected and Access Personal Information
- Right to Know What Personal Information is Sold or Shared, and to Whom
- Right to Opt-Out of the Sale or Sharing of Personal Information
- Right to Limit Use and Disclosure of Sensitive Personal Information
- Right of Non-Retaliation

If you are a California resident and wish to exercise any of these rights, please contact us using the information provided in our Privacy Notice.

b. Rights for EU/EEA/UK Residents (GDPR & UK GDPR)

Under the General Data Protection Regulation (GDPR) and UK GDPR, individuals in the European Economic Area (EEA), United Kingdom (UK), and Switzerland have the following rights:

- Right to Access

- Right to Rectification
- Right to Erasure ("Right to be Forgotten")
- Right to Restriction of Processing
- Right to Data Portability
- Right to Object
- Right to Withdraw Consent
- Right to Lodge a Complaint

To exercise your GDPR rights or inquire about how we process your data, please contact us through the details provided in our Privacy Notice.

c. Rights for Canadian Residents (PIPEDA)

If you are a resident of Canada, your personal information is protected under the Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial privacy laws. Your rights under PIPEDA include:

- Right to Access
- Right to Correction
- Right to Withdraw Consent
- Right to Challenge Compliance

Under PIPEDA, we process personal information based on:

- Implied or Express Consent – We may rely on either express consent (e.g., signing a form) or implied consent (where the purpose is obvious).
- Legal Exceptions – In some cases, we may process personal data without consent, such as for fraud prevention, legal compliance, or investigations.

16. Federal Trade Commission (FTC)

HqO is subject to the investigatory and enforcement powers of the FTC.

17. Arbitration

HqO is obligated to arbitrate claims and follow the terms as set forth in Annex I of the DPF Principles, provided that an individual has invoked binding arbitration by delivering notice to HqO and following the procedures and subject to conditions set forth in Annex I of Principles.

If the dispute remains unresolved after ADR, individuals may invoke binding arbitration under the DPF Panel's rules, provided they have completed all prior resolution steps.

18. Accountability for Onward Transfers Consistent with the DPF Principles.

HqO may transfer personal information to third parties, including transfers from one country to another. We will only disclose an individual's personal information to third parties under one or more of the following conditions:

- The disclosure is to a third party providing services to HqO, or to the individual, in connection with the operation of our business, and as consistent with the purpose for which the personal information was collected. We maintain written contracts with these third parties and require that these third parties provide at least the same level of privacy protection and security as required by the DPF Principles. To the extent provided by the DPF Principles, HqO remains responsible and liable under the DPF Principles if a third party that it engages to process personal information on its behalf does so in a manner inconsistent with the DPF Principles, unless HqO proves that it is not responsible for the matter giving rise to the damage;
- With the individual's permission to make the disclosure;
- Where required to the extent necessary to meet a legal obligation to which HqO is subject, including a lawful request by public authorities and national security or law enforcement obligations and applicable law, rule, order, or regulation;
- Where reasonably necessary for compliance or regulatory purposes, or for the establishment of legal claims.

19. Contact Information

HqO may update this policy periodically to reflect regulatory changes or operational adjustments. Any material changes will be communicated via our website or direct user notifications.

If you are a resident of the United Kingdom or European Economic Area, please note that we have appointed an EU data protection representative. For further inquiries, please contact our Data Protection Officer (DPO) at: legal@hqo.co.

(D) HqO Privacy Policy for HqO Business Customers

If you are a business customer of HqO, HqO, Inc., is the controller of your information collected from and about you as part of our business customer services (“HqO Business Customer Services”).

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, HqO, Inc. commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner’s Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF in the context of the employment relationship. This applies to parts A, B, and C of the Privacy Policy.

Please read this Privacy Policy to understand how we may process your information via your use of our HqO Business Customer Services. If you do not agree with how we process your information, please do not use the HqO Business Customer Services. If you are a business customer that also uses the HqO Services through our App, or that uses our Site, please also see the privacy policies relevant to those services.

1. Information We Collect

When you interact with us as a user of the HqO Business Customer Services, we may collect information from and about you, as further described below:

Information That You Provide: We collect information from you when you voluntarily provide it, such as when you contact us with inquiries, respond to one of our surveys, provide it at a conference or event, or otherwise use the HqO Business Customer Services. This information may include your name, business contact information, and title.

Research and Analytics Data: In an ongoing effort to better understand and serve the users of HqO Business Customer Services, HqO often conducts research on its customer demographics, interests and behavior based on the information you provide to us. This research may be compiled and analyzed on an aggregate and/or de-identified basis, in which case HqO may share this aggregated and/or de-identified data with its affiliates, agents and business partners. This aggregate and/or de-identified information cannot be used to identify you personally. HqO may also disclose aggregated user statistics to describe our services to current and prospective business partners, and to other third parties for other lawful purposes.

2. Data Retention Policy

HqO retains personal data only for as long as necessary to fulfill the purposes for which it was collected or as required by applicable law. Specifically:

- Client and customer data: Retained for up to five years post-contract expiration, unless legal retention is required.
- HR data: Retained for seven years after employment termination.
- Marketing and analytics data: Retained for two Years, unless the individual opts out sooner.

Once data is no longer needed, HqO securely deletes or anonymizes it.

3. Security Measures

HqO takes appropriate technical and organizational measures to protect personal data against loss, misuse, unauthorized access, disclosure, alteration, and destruction. Our security protocols include:

- Data encryption (AES-256 for stored data, TLS 1.2+ for transmitted data).
- Access control measures to restrict unauthorized personnel from accessing sensitive data.
- Incident response procedures for detecting, containing, and mitigating data breaches.

4. User Rights and Opt-Out Mechanisms

HqO respects individuals' rights under DPF and applicable data protection laws. Users may exercise the following rights:

- Right to access & correct Data: Users can request a copy of their data and request corrections if inaccurate.
- Right to delete data: Users can request deletion of their personal data where no legal retention is required.
- Right to limit use & Disclosure (opt-out). Users can opt-out of marketing communications via an unsubscribe link in emails or by contacting legal@hgo.co.

Requests can be submitted through our Privacy Request Form or via legal@hgo.co.

5. Enforcement and Dispute Resolution

HqO is committed to resolving complaints regarding our collection and use of personal data in compliance with the DPF Principles. Users may submit complaints to HqO directly via legal@hqo.co.

We aim to resolve any dispute you may raise within 45 days.

6. Our Use of Your Information and Legal Bases for Processing Information

We process the information you provide to us to enable us to provide the HqO Business Customer Services to you, to ensure compliance with local legal and regulatory requirements, and for the purposes of our legitimate business interests, including to:

- enable us to carry out our obligations to provide you with the information, products and services that you request from us;
- enable us to respond to an inquiry or other request you make when you contact us, including for customer services support;
- notify you about any changes to the HqO Business Customer Services;
- enable us to issue a notice or corrective action to you in relation to any of the HqO Business Customer Services, if required;
- help us improve the content and functionality of the HqO Business Customer Services, and to better understand and analyze how you use our Services;
- detect security incidents, and protect against malicious, deceptive, fraudulent, or illegal activity;
- troubleshoot and debug HqO Business Customer Services errors;
- provide you with information about other services which we believe will be of interest to you similar to those that you have already purchased or inquired about, as described in the “Marketing” section below.

We process personal information under the following legal bases, depending on the applicable jurisdiction:

- GDPR / UK GDPR: We rely on legitimate interest, contract performance, legal obligation, and consent, as required, to process personal data.
- CCPA: We process data for business purposes, consumer consent, and service provision, in compliance with California privacy laws.
- PIPEDA: We rely on implied or express consent, except where legal exceptions apply.
- Australia (APPs): We collect personal information directly where necessary for our business operations, relying on individual consent where required under the Australian Privacy Act.

7. Marketing

HqO and its affiliates (see Schedule I for list of affiliates) (the “HqO Related Companies”) may also use your information to contact you via email, phone, or postal mail with promotional materials in the future to tell you about services we believe will be of interest to you, in accordance with applicable law.

Note: References to 'HqO and its affiliates' refer to operational business relationships. Only HqO, Inc. is certified under the DPF.

In our promotional emails, there will be instructions explaining how to “opt-out” of receiving them in the future, if you would like. In addition, if at any time you wish not to receive any future promotional communications or you wish to have your name deleted from our mailing lists, please contact us as indicated below. Please note that it may take time to process your request, consistent with our legal obligations. Also, after you have opted out, you may continue to receive non-promotional, transactional communications from us.

8. Our Disclosure of Your Information

We may share your information with certain third parties, as set forth below:

- **Business Transfers:** As we develop our business, we might sell or buy some or all of our businesses or assets. In the event of a corporate sale, merger, reorganization, dissolution or similar event, your information may be part of the transferred assets.
- **Related Companies:** We may also share your information with our HqO Related Companies for purposes consistent with this Privacy Policy.
- **Agents, Consultants and Related Third Parties:** We, like many businesses, sometimes hire other companies to perform certain business-related functions on our behalf. Examples of such functions include hosting the HqO Services, mailing information, sales and marketing, shipping and fulfillment, maintaining databases, and processing payments. When we employ another company to perform a function of this nature, we only provide them with the information that they need to perform their specific function.
- **Legal Requirements:** We may disclose your information if required to do so by law or in the good faith belief that such action is necessary to (i) comply with a legal obligation, (ii) protect and defend our rights or property, (iii) act in urgent circumstances to protect the personal safety of users of the HqO Services or the public, or (iv) protect against legal liability.

9. Storing Your Information

Your information collected via the HqO Business Customer Services will be stored on servers located in the United States, European Union and other locations that may have different data protection laws than in your jurisdiction. This includes by individuals or service providers engaged in, among other things, administration of an enquiry or request you make via the HqO Business Customer Services, or the provision of support services. By using the HqO Business Customer Services, you acknowledge that your information will be stored and processed in the United States, European Union and potentially other global locations.

10. Data Privacy Framework Principles

a. Data Privacy Framework (DPF) for EU-U.S. & UK-U.S. Transfers

HqO complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. These frameworks govern the processing of Personal Data (as defined by applicable EU, UK, and Swiss data protection laws) transferred to the United States from these regions.

HqO has certified to the U.S. Department of Commerce that it adheres to the DPF Principles with respect to the processing of personal data received under these frameworks. If any conflict arises between the terms in this privacy policy and the DPF Principles, the DPF Principles shall govern.

To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>.

b. Dispute Resolution & Complaints Handling

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, HqO, Inc. commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO), and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.

On 4 June 2021, the Commission issued modernised standard contractual clauses under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the

GDPR).

These modernised SCCs replace the three sets of SCCs that were adopted under the previous Data Protection Directive 95/46. Consequently, we are relying on standard contractual clauses (based on the clauses published [here](#), a copy of which can be obtained by contacting us at legal@hgo.co.) for transfers of personal data from the EEA.

c. Compliance with PIPEDA

HqO complies with the Personal Information Protection and Electronic Documents Act (PIPEDA) and its contractual obligations for international transfers.

HqO implements contractual safeguards in accordance with PIPEDA, including binding contractual clauses with our service providers.

We conduct periodic assessments to verify that our international data recipients comply with these contractual obligations and maintain adequate data protection measures.

Canadian users who have concerns about international data transfers may contact us at legal@hgo.co for more details.

d. Compliance with APP 8.1

HqO complies with the Australian Privacy Act 1988 and the Australian Privacy Principles (APPs).

HqO meets Australian legal requirements by:

- Implementing contractual safeguards with overseas recipients.
- Conducting risk assessments to evaluate whether the recipient provides an adequate level of data protection.
- Obtaining consent where necessary before transferring sensitive personal data internationally.
- If you are an Australian resident and have concerns about how your personal data is handled under APP 8.1, you can contact us at legal@hgo.co.

e. Standard Contractual Clauses (SCCs) for International Data Transfers (GDPR/EEA/UK)

On 4 June 2021, the European Commission issued modernized Standard Contractual Clauses (SCCs) under the GDPR for data transfers from controllers or processors in the EU/EEA/UK to non-EU/EEA/UK recipients.

These modernized SCCs replace previous SCCs that were based on the Data Protection Directive 95/46.

HqO relies on SCCs as an approved mechanism for transferring personal data from the EEA/UK to third countries (including the U.S.).

A copy of the Standard Contractual Clauses (SCCs) used by HqO is available upon request via legal@hgo.co.

11. Data Retention

We will only retain your information for as long as necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for your information, we consider the amount, nature, and sensitivity of the information, the potential risk of harm from unauthorized use or disclosure of your information, the purposes for which we process your information and whether we can achieve those purposes through other means, and the applicable legal requirements.

12. Exclusions

This Privacy Policy does not apply to information collected by HqO other than information collected through the HqO Business Customer Services. This Privacy Policy will not apply to any unsolicited information you provide to HqO through any other means. This includes, but is not limited to, any ideas for new products or modifications to existing products, and other unsolicited submissions (collectively, "Unsolicited Information"). All Unsolicited Information will be deemed to be non-confidential and HqO will be free to reproduce, use, disclose, and distribute such Unsolicited Information to others without limitation or attribution.

13. Security

HqO takes steps to protect the information provided via the Site and HqO Services from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. However, no Internet or e-mail transmission is ever fully secure or error free. Please keep this in mind when disclosing any information to HqO.

14. Changes to HqO's Privacy Policy

Our business, and applicable legal requirements, may change from time to time. As a result, at times it may be necessary for HqO to make changes to this Privacy Policy. HqO reserves the right

to update or modify this Privacy Policy at any time in accordance with our legal obligations. Please review this policy periodically. This Privacy Policy was last updated on the date indicated above. Your continued use of the Site or HqO Services after any changes or revisions to this Privacy Policy will indicate your agreement with the terms of such revised Privacy Policy.

15. Your Rights

To keep your information accurate, current, and complete, please contact us as specified below. We will take reasonable steps to update or correct your information in our possession in accordance with applicable law.

You may have the right to:

- request access to your Personal Data we hold about you, request we correct any inaccurate Personal Data we hold about you;
- request we delete any Personal Data we hold about you;
- restrict the processing of Personal Data we hold about you; object to the processing of Personal Data we hold about you;
- and/or receive any Personal Data we hold about you in a structured and commonly used machine-readable format or have such Personal Data transmitted to another company.

We may ask you for additional information to confirm your identity and for security purposes, before disclosing information requested to you. We will process any request in line with any local laws and our policies and procedures. If you are located in the EEA or United Kingdom, you have the right to lodge a complaint about how we process your Personal Data with the supervisory authority in your country.

If you wish to exercise any of your rights, please contact us using the information provided in the section.

16. Privacy Rights

a. Your Privacy Rights for California Residents (CCPA/CPRA)

Under the CCPA and CPRA, California residents have the following rights:

- Right to Request and Receive Personal Information Disclosures
- Right to Delete Personal Information
- Right to Correct Inaccurate Personal Information
- Right to Know What Personal Information is Being Collected and Access Personal Information
- Right to Know What Personal Information is Sold or Shared, and to Whom
- Right to Opt-Out of the Sale or Sharing of Personal Information
- Right to Limit Use and Disclosure of Sensitive Personal Information
- Right of Non-Retaliation

If you are a California resident and wish to exercise any of these rights, please contact us using the information provided in our Privacy Notice.

b. Rights for EU/EEA/UK Residents (GDPR & UK GDPR)

Under the General Data Protection Regulation (GDPR) and UK GDPR, individuals in the European Economic Area (EEA), United Kingdom (UK), and Switzerland have the following rights:

- Right to Access
- Right to Rectification
- Right to Erasure ("Right to be Forgotten")
- Right to Restriction of Processing
- Right to Data Portability
- Right to Object
- Right to Withdraw Consent
- Right to Lodge a Complaint

To exercise your GDPR rights or inquire about how we process your data, please contact us through the details provided in our Privacy Notice.

c. Rights for Canadian Residents (PIPEDA)

If you are a resident of Canada, your personal information is protected under the Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial privacy laws. Your rights under PIPEDA include:

- Right to Access
- Right to Correction

- Right to Withdraw Consent
- Right to Challenge Compliance

Under PIPEDA, we process personal information based on:

- Implied or Express Consent – We may rely on either express consent (e.g., signing a form) or implied consent (where the purpose is obvious).
- Legal Exceptions – In some cases, we may process personal data without consent, such as for fraud prevention, legal compliance, or investigations.

13. Federal Trade Commission (FTC)

HqO is subject to the investigatory and enforcement powers of the FTC.

14. Arbitration

HqO is obligated to arbitrate claims and follow the terms as set forth in Annex I of the DPF Principles, provided that an individual has invoked binding arbitration by delivering notice to HqO and following the procedures and subject to conditions set forth in Annex I of Principles.

If the dispute remains unresolved after ADR, individuals may invoke binding arbitration under the DPF Panel's rules, provided they have completed all prior resolution steps.

15. Accountability for Onward Transfers Consistent with the DPF Principles

HqO may transfer personal information to third parties, including transfers from one country to another. We will only disclose an individual's personal information to third parties under one or more of the following conditions:

- The disclosure is to a third party providing services to HqO, or to the individual, in connection with the operation of our business, and as consistent with the purpose for which the personal information was collected. We maintain written contracts with these third parties and require that these third parties provide at least the same level of privacy protection and security as required by the DPF Principles. To the extent provided by the DPF Principles, HqO remains responsible and liable under the DPF Principles if a third party that it engages to process personal information on its behalf does so in a manner inconsistent with the DPF Principles, unless HqO proves that it is not responsible for the matter giving rise to the damage;
- With the individual's permission to make the disclosure;
- Where required to the extent necessary to meet a legal obligation to which HqO is subject, including a lawful request by public authorities and national security or law enforcement obligations and applicable law, rule, order, or regulation;

- Where reasonably necessary for compliance or regulatory purposes, or for the establishment of legal claims.

16. Contact Information

HqO may update this policy periodically to reflect regulatory changes or operational adjustments. Any material changes will be communicated via our website or direct user notifications.

If you are a resident of the United Kingdom or European Economic Area, please note that we have appointed an EU data protection representative. For further inquiries, please contact our Data Protection Officer (DPO) at: legal@hqo.co.

Schedule I - Affiliates of HqO, Inc.

1. HqO UK Limited (UK)
2. Office App Limited (UK)
3. Office App (Netherlands)
4. Leesman Limited (UK)

In compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), HqO, Inc. commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO), and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the DPF.