PRIVACY POLICY

LogaXP

Effective November1, 2023

Protecting your private information is our priority. This Statement of Privacy applies to the LLC and its affiliates (referred to as “LogaXP,” “logaXP.com,” the “Company,” “we,” “us,” or “our”) and governs data collection and usage. The LogaXP website is an Online booking software site. By using the LogaXP website (the “Site”), you consent to the data practices described in this statement.

SECTIONS OF PRIVACY POLICY

- Collection of your Personal Information
- Use of Cookies, Web Beacons, and Log Files
- Security of your Personal Information
- Children's Privacy
- For California Visitors Only: Your California Privacy Rights
- Privacy Information for Visitors from the EU
- Visitors from Outside the United States — Cross-Border Transfer
- Opt-Out & Unsubscribe
- Changes to this Statement
- Contact Information

COLLECTION OF YOUR PERSONAL INFORMATION

Category of Personal Information Collected	Source of Information	Purpose for Collection	Categories of Recipients
Contact information, such as your name, address, email address, telephone numbers, or other contact information provided by you when you register	From you	To fulfill your requests for services and information; to improve our website’s functionality; to improve our services; to communicate with you; to provide you with information about products and services that might interest you; and for internal business analysis or other business purposes	LogaXP; LogaXP’s trusted partners (to help perform statistical analysis, send you email or postal mail, provide customer support, or arrange for deliveries)

Login information, such as password and password reminder questions and answers	From you	To enable you to access the Site	This information is not shared outside LogaXP.
Payment information, such as card type, card issuer, credit or debit card number, expiration date, CVV code, billing address, bank account number, and other bank account details	From you and your payment card issuer	To check that the right person is using the right card or account; to meet the requirements of the card brands or account issuers, and to make sure we are paid for what you buy	Our card processor stores all credit card information. They conduct the credit card transactions using commercially reasonable security precautions, controls, policies, and procedures, consistent with generally accepted data processing standards in the financial services industry. We only store a record that the transaction took place and the amount you donated in connection with your account information.
Information you provide about a third party: if you send someone else a communication from the Site, we may collect information such as that person's name, telephone number, email, and/or address	From you	To communicate with the person at the address which you have requested	LogaXP; certain authorized third-party vendors who help us provide specialized services (such as customer support, email and text message deployment, business analytics, marketing, and payment and data processing)
Information automatically collected from your browser, including the full URL clickstream to, through and from our website (including date and time); URL requests, destination IP addresses, or device configuration details; and website pages and listings you viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-	From you and from our website technology's interaction with your browser or devices and cookies tracking the pages you visit	To improve our Site, services, customer service, and user experience	LogaXP; certain authorized third-party vendors who help us provide specialized services (such as customer support, email and text message deployment, business analytics, marketing, and payment and data processing)

overs), and methods used to browse away from the page			
Device information, including log files, MAC address, IP address, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform, device type, and device identifiers	From you and from our website technology's interaction with your browser or devices	To improve our Site, services, customer service, and user experience	LogaXP; certain authorized third-party vendors who help us provide specialized services (such as customer support, email and text message deployment, business analytics, marketing, and payment and data processing)
Public information you provide, such as through LogaXP's public message boards	From you	To analyze the use of LogaXP and information about visitors to our Site; to understand and improve our offerings, advertising and programming; for research, analytical and other business purposes; in accordance with our sharing policies, to produce anonymous or aggregated data and statistics that might help third parties develop their own products and service offerings; and for any other purposes disclosed to you at the time We collect your information or pursuant to your consent	LogaXP; certain authorized third-party vendors who help us provide specialized services (such as customer support, email and text message deployment, business analytics, marketing, and payment and data processing); third parties (for development of products and service offerings based on anonymous or aggregated data)
Legal information, such as contact information, fraud checks or flags raised about your transactions, the payment card you want to use, payment card refusals, suspected crimes, complaints, claims and accidents	From you, the police, crime and fraud prevention agencies, payment card providers, the public, regulators, your and our professional advisors and representatives	To protect you, other customers and our business against criminal activities and risks; to make sure we understand and can meet our legal obligations to you and others and can defend ourselves	LogaXP; our service providers who help us with fraud protection and credit risk reduction; law enforcement and other governmental authorities in accordance with applicable law

Communications from you, such as emails you send us, feedback forms you fill out, and phone calls, chats, or other communications with you (we will inform you at the start of video and phone calls that the call is recorded).	From you	To handle your requests and to contact you when necessary or requested, including responding to your questions and comments and providing customer support	LogaXP; certain authorized third-party vendors who help us provide specialized services (such as customer support, email and text message deployment, business analytics, and marketing)
Third party social media information: when you choose to interact with us or log in via social media platforms (such as Facebook, Twitter, and LinkedIn) we may automatically collect information such as your personally identifiable information list, the profile pictures of the contact list, education, work history, events, relationship status, likes, gender, location, URL, biography, any additional image, or information. We may also collect your communications with us through the third-party social media platforms.	From you	To authenticate your identity and link your social media profile information to your LogaXP account	LogaXP; certain authorized third-party vendors who help us provide specialized services (such as customer support, email and text message deployment, business analytics, marketing, and payment and data processing)

Disclosure to Third Parties. We do not display your contact information publicly on our site or disclose personally identifiable information to third parties, except for when (1) we have your permission to make the disclosure, (2) the disclosure is necessary for the purpose for which the information was obtained, (3) a third party is assisting us to provide or manage the services or website, or (4) where otherwise stated in this policy. We also may disclose information where permitted by applicable law or when the disclosure is necessary, in our sole discretion, for the establishment or maintenance of legal claims or legal compliance, to satisfy any law, regulation, subpoena or government request, or in connection with litigation.

Business Transfers. In the event we are acquired by or merged or consolidated into another entity, or if there is a sale of our assets, your information may be transferred to the entity acquiring us or our assets or the entity that survives the merger or consolidation. You acknowledge and agree that in the foregoing circumstances, your information may be disclosed to such third party.

USE OF COOKIES, WEB BEACONS, AND LOG FILES

Cookies

A cookie is a small amount of data, which often includes an anonymous unique identifier, that is sent to your browser from a web site's servers and stored on your computer's hard drive. Cookies are required for our service. We use cookies to track and record user session information. Some examples include keeping you logged into your account while keeping your session secure, views of specific pages or modals, and the number of password reset requests. We do not use permanent cookies but will require users to log in periodically to our site in order to help protect your account information.

Web Beacons

Additionally, emails we send may contain a bit of code known as a "web beacon." This code allows us to understand the time and date of when a user has opened an email and when he/she has utilized a link within the email to visit a website. Our web beacons do not collect personally identifiable information and you may disable our web beacons. Please see your email client for more information regarding disabling web beacons.

Log Files

Like many other web sites, the Company makes use of log files. The information inside the log files includes internet protocol (IP) addresses, type of browser, Internet Service Provider (ISP), date/time stamp, referring/exit pages, and number of clicks to analyze trends, administer the site, track user's movement around the site, and gather demographic information.

SECURITY OF YOUR PERSONAL INFORMATION

We take precautions but cannot provide guarantees. We do our best to secure your data through the programming of our services and the use of security measures that we deem appropriate for the type of data provided. However, we cannot completely guarantee that no part of our system or site will ever fail or be compromised. If you ever suspect that our site or services has contributed to your personal information being compromised, please contact us immediately so that we can investigate and try to resolve the matter.

CHILDREN'S PRIVACY

Our Site is not directed to individuals under the age of 13, and we request that individuals under 13 not provide personal data to LogaXP. We do not knowingly collect personal information from persons under the age of thirteen (13) without verifiable parental consent. If we learn that a child under the age of thirteen (13) has submitted personally identifiable information online without parental consent, we will take all reasonable measures to delete such information from our databases and to not use such information for any purpose (except where necessary to protect the safety of the child or others as required or allowed by law). If you become aware of any personally identifiable information, we have collected from children under thirteen (13), please contact us at support@LogaXP.com. If you are a

member or contact of one of our customers, you should review their privacy policy to determine their privacy practices with respect to children's data.

FOR CALIFORNIA VISITORS ONLY: YOUR CALIFORNIA PRIVACY RIGHTS.

California residents who provide personal information in obtaining products or services for personal, family, or household use are entitled to request and obtain from us once a calendar year information about the customer information we shared with third parties for their own direct marketing purposes, including the categories of information and the names and addresses of those businesses with which we have shared such information. As discussed elsewhere in this Privacy Policy, we do not currently share the personal information of California residents with third parties for their own direct marketing purposes. However, if you have further questions about our privacy practices and compliance with California law, please contact us as explained below.

If you are a California resident, the California Consumer Privacy Act provides you with the following rights with respect to your personal information:

The right to request to know the categories or specific pieces of personal information we have collected, used, disclosed, and sold about you. To submit a request to know, you may email us at support@LogaXP.com or visit https://www.LogaXP.com/contact.html. You also may designate an authorized agent to make a request for access on your behalf on our website at https://www.LogaXP.com/contact.html.

The right to request that we delete any personal information we have collected about you. To submit a request for deletion, you may email us at support@LogaXP.com or visit https://www.LogaXP.com/contact.html. You also may designate an authorized agent to make a request for deletion on your behalf on our website at https://www.LogaXP.com/contact.html.

When you exercise these rights and submit a request to us, we will verify your identity by asking you to log in to your account if you have one with us. Or if you do not, we may ask for your email address and require additional. We also may use a third-party verification provider to verify your identity.

The fact that you have elected to exercise these rights will have no adverse effect on the price and quality of our Services.

The Company does not and will not sell your personal information.

Minors Under 18 in California

Minors under 18 years of age in California may have the Personal Information that they provide to us through the Site deleted by sending an email requesting deletion to [email address]. Please note that,

while we make reasonable efforts to comply with such requests, deletion of your personal information does not ensure complete and comprehensive removal of that data from all systems.

California Do Not Track Disclosure

Some Internet browsers include the ability to transmit “Do Not Track” signals, which is a privacy preference that users can set in some web browsers, allowing users opt out of tracking by websites and online services. Since uniform standards for “Do Not Track” signals have not been adopted, LogaXP does not process or respond to “Do Not Track” signals.

VISITORS FROM OUTSIDE THE UNITED STATES — CROSS-BORDER TRANSFER

The Website is hosted in the United States. If you are visiting the Website from outside the United States, your information may be transferred to, stored, and processed in the United States or other countries in accordance with this privacy policy. The data protection and other applicable laws of the United States or other countries may not be as comprehensive as those laws or regulations in your country or may otherwise differ from the data protection or consumer protection laws in your country. Your information may be available to government authorities under lawful orders and law applicable in such jurisdictions. By using the Website and/or providing personal information to us, you consent to transfer your information to our facilities as described in this Privacy Policy.

OPT-OUT & UNSUBSCRIBE

You may have the opportunity to receive certain communications from us related to our website or Services. If you provide us with your email address in order to receive communications, you can opt out at any time by using the unsubscribe links at the bottom of our emails.

Please note that certain emails may be necessary to provide you with our Services. You will continue to receive these emails, if appropriate, even if you unsubscribe from our optional communications.

CHANGES TO THIS STATEMENT

The Company will occasionally update this Privacy Policy to reflect company and customer feedback. The Company encourages you to periodically review this Statement to be informed of how The Company is protecting your information.

If any of the items above are unclear or you have further questions, or if you would like to request a copy of this Privacy Policy in a different format, please contact us at:

Loga System

LogaXP Address:

Email Address: support@logaXP.com

Telephone number:

GDPR

Information on how LogaXP meets GDPR security regulations.

Like many other companies, LogaXP has reviewed its company-wide compliance strategy with respect to the EU General Data Protection Regulation (GDPR), which came into effect from 25th May 2018.

In doing so, LogaXP completed an audit of all data flowing in and out of our organization, either in our capacity as a Data Controller or as a Data Processor.

As a result, we have reviewed and updated our Privacy Policy and Cookie Policy; ensured we obtain consent before collecting personal data of our customers; provide access to that data and provide the right to be forgotten in accordance with our Privacy Policy. We have either signed Data Processing Addendums with relevant third-party service providers or moved away from non-compliant providers.

LogaXP now offers a GDPR compliant Data Processing Addendum to our standard License Agreement so that customers can use our services in a GDPR compliant manner, and we have executed Data Processing Addendums with our sub-processors.

We are committed to a process of continual improvement of our privacy and security measures, notifying regulators of personal data breaches and promptly communicating any such breaches to our customers.

GDPR - FAQ

What is the GDPR?

The General Data Protection Regulation (GDPR) is a new European privacy law. The GDPR increases protection around the processing of personal data of EU data subjects by applying a single data protection law that is binding throughout each member state of the EU.

Who does the GDPR apply to?

The GDPR applies to any organization, whether or not they are established in the EU, that is processing personal data of EU data subjects.

Is LogaXP a Data Controller or Data Processor?

Under the GDPR, LogaXP is both a Data Controller and a Data Processor.

Data Controller – LogaXP acts as a data controller when we collect and store accounts and contact information of our customers.

Data Processor – LogaXP acts as a data processor when our customers use LogaXP services to process personal data. Under these circumstances, our customer may act as a data controller or data processor, and LogaXP acts as a data processor or sub-processor.

Can I use the LogaXP to Process Personal Data?

Yes. If you intend to schedule documents that may contain Personal Data, you should:

Sign the Data Processing Addendum to our standard License Agreement.

Use the LogaXP guidelines in accordance with: Guidelines for Using LogaXP Cloud Services in a GDPR-Compliant Manner

How do I enter the Data Processing Addendum with LogaXP?

Please send an email to privacy@LogaXP.com that specifies:

Your personal name

Your position

Company name

We will then send you a copy of the Data Processing Addendum that you can review and sign electronically.

What technical and organizational measures does LogaXP have in place?

In response to Article 28 and 32 of the GDPR, we outline the technical and organizational measures we use to ensure the ongoing confidentiality, integrity, availability, and resilience of the LogaXP Cloud service, here: Security Measures

WHY LOGAXP?

LogaXP was designed with a clear focus on addressing the needs of businesses that have previously encountered challenges with other appointment scheduling systems. Launched in 2022, Ged is dedicated to serving businesses and organizations with sophisticated appointment scheduling requirements, offering a reliable and feature-rich solution.

HIPAA BUSINESS ASSOCIATE ADDENDUM

Last updated: November 1th, 2023

Contact Us with any questions!

1. HIPAA COMPLIANCE

The Federal Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (45 C.F.R. Parts 160-164) ("HIPAA") sets forth standards for protecting the privacy of individually identifiable health information. HIPAA's requirements become effective as of April 14, 2003. Pursuant to HIPAA, Business User on behalf of itself and its related covered entities including all entities controlled, partially controlled, owned, partially owned, managed or partially managed by Business User (referred to in this Addendum as the "Covered Entity") is required to enter into Business Associate Agreements with all of its contractors, agents and related and unrelated third parties that perform a function or activity on behalf of such Covered Entity that involves providing contractors, agents, and related and unrelated third-parties with individually identifiable health information. This Addendum is made a part of any Agreements executed between the parties (the "Agreement"). This Addendum is intended to comply with the Covered Entity's requirements under HIPAA. The Parties to the Agreement hereby acknowledge and agree that LLC is a "Business Associate" of Covered Entity as that term is defined by HIPAA. For purposes herein, Business Associate and Covered Entity shall be collectively referred to as the "Parties." Capitalized terms used in this Addendum and not otherwise defined herein shall have the meanings set forth in HIPAA, which definitions are hereby incorporated by reference.

2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

(a) Business Associate agrees to use or disclose Protected Health Information ("PHI") received from or on behalf of Covered Entity or created for Covered Entity only as permitted or required by this Addendum, the Agreement or as required by law.

(b) Business Associate agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any electronic PHI that it creates, receives, maintains or transmits on behalf of the Covered Entity. The Business Associate shall document and keep its documentation with respect to these security measures available for inspection, upon reasonable request.

(c) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Addendum.

(d) Business Associate agrees to report to Covered Entity any security incident (including any attempted or actual unauthorized access or breach of PHI) and/or any use or disclosure of the PHI not provided for by this Addendum of which it becomes aware.

(e) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by Business Associate on behalf of, Covered Entity agrees to the same restrictions and conditions that apply through this Addendum to Business Associate with respect to such information.

(f) Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or to the Secretary, in a time and manner mutually agreed by the Parties or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

(g) Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. §164.528.

(h) Business Associate agrees to provide to Covered Entity, in time and manner mutually acceptable to the Parties, information collected in accordance with Section 2(g) of this Addendum, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. §164.528.

(i) To the extent that Business Associate has PHI in a Designated Record Set, Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner mutually agreed by the Parties, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the Covered Entity's requirements under 45 C.F.R. §164.524.

(j) To the extent that Business Associate has PHI in a Designated Record Set, Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. Section Code 164.526 at the request of Covered Entity, and in the time and manner mutually agreed by the Parties.

3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

Except as otherwise limited in this Addendum, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Agreement.

(a) Except as otherwise permitted in this Addendum, Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(b) Except as otherwise permitted in this Addendum, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. §164.504(e)(2)(i)(B).

(c) Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with §164.502(j)(1).

4. OBLIGATIONS OF COVERED ENTITY

(a) Upon request, Covered Entity shall provide Business Associate with a copy of its Notice of Privacy Practices.

(b) Covered Entity shall notify Business Associate of any limitations in its notice of privacy practices, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

(c) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

(d) Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

5. TERM AND TERMINATION.

(a) Term. The Term of this Addendum shall be effective upon execution of the Addendum by both Parties and, except for the rights and obligations set forth in this Addendum specifically surviving termination, shall terminate upon the termination of the final Agreement executed between the Parties.

(b) Termination for Cause. In addition to any termination provisions otherwise set forth in the Agreement, upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

(i) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Addendum and the Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity.

(ii) Immediately terminate this Addendum and the Agreement if Business Associate has breached a material term of this Addendum and cure is not possible; or

(iii) If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

(c) Effect of Termination.

(i) Except as provided in paragraph (ii) below of this section, upon termination, for any reason, of this Addendum or the final Agreement executed between the Parties, Business Associate shall return or destroy all PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity. Business Associate shall retain no copies of the PHI.

(ii) In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Business Associate shall extend the protections of this Addendum to such PHI and

permit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

6. MISCELLANEOUS.

(a) Regulatory References. A reference in this Addendum to a section in the Privacy Rule means the section as in effect or as amended.

(b) Amendment. The Parties agree to take such action as is necessary to amend this Addendum from time to time as is necessary for Covered Entity to comply with the requirements of HIPAA.

(c) Survival. The respective rights and obligations of Business Associate under Section 6(c) of this Addendum shall survive the termination of this Addendum and any Agreements executed between the Parties.

(d) Interpretation. Any ambiguity in this Addendum shall be resolved to permit Covered Entity to comply with the Privacy Rule.

(e) Conflicts. To the extent that there is any conflict between the provisions of this Addendum and the Agreement, the provisions of this Addendum shall control. To the extent that the law of the state in which the Covered Entity does business is more stringent than Federal law regarding privacy issues, the law of such state shall control, unless such state law is expressly preempted by the Federal law.

(f) Response to Subpoenas. In the event that Business Associate receives a subpoena or similar notice or request from any judicial, administrative, or other party arising out of or in connection with this Addendum or the Agreement, including, but not permitted to, any unauthorized use or disclosure of PHI or any failure in Business Associate's security measures, Business Associate shall promptly forward a copy of such subpoena, notice or request to Covered Entity.