SCELTA PRIVACY POLICY

Effective 25-03-01

Welcome to Scelta's Privacy Policy. This document complements our Terms of Service by delving deeper into our privacy practices, embodying our staunch commitment to the protection and respectful handling of your information. Here, we outline how we collect, use, manage, and secure the data you entrust to us, guided by the principles of integrity, legal compliance, and mutual trust. Our practices are designed to uphold fundamental privacy rights, reflecting our alignment with the spirit and the letter of laws such as the Personal Information Protection and Electronic Documents Act (PIPEDA) and other applicable privacy legislation.

1. OVERVIEW

Purpose: This Privacy Policy outlines how Scelta collects, uses, manages, and protects the information provided to us by users of our services. Our commitment is to ensure the confidentiality and integrity of your information, adhering to legal standards and fostering trust and transparency in our interactions.

Scope and Application: This policy applies to all information Scelta collects through our services and platforms. It encompasses interactions with our software, website, and any digital or physical engagements where users provide personal or business information to Scelta.

Legal Status of this Privacy Policy: This Privacy Policy is an essential component of Scelta's contracts with its clients and is incorporated by reference as a part of Scelta's contractual Terms of Service. It is a stand-alone document because of the issues of:

- privacy,
- compliance with privacy law,
- privacy policy disclosure, and
- transparency,

represent fundamental human rights in a data-driven world. The laws of Canada, in particular the Personal Information Protection and Electronic Documents Act (PIPEDA), and the laws of the Province of Ontario govern this Privacy Policy.

2. DEFINITIONS

Scelta: refers to Scelta Customs Inc., an Ontario Business Corporation governed by the laws of Canada and the Province of Ontario.

Individual: Any identifiable person whose personal information is collected, used, or disclosed by Scelta in its commercial activities or through its services in the course of commercial activities by its clients and their authorized users.

Subprocessors: Third-party services engaged by Scelta to process information on behalf of Scelta and its Clients in alignment with the definitions and obligations outlined in these Terms of Service and the Privacy Policy.

Personal Information: is defined in the Personal Information Protection and Electronic Documents Act (PIPEDA), its guidance specifically and generally by the evolving global understanding of privacy protection. It includes any factual or subjective data, recorded or not, about an identifiable individual. Within personal information is a further category called sensitive personal information that requires additional protection. Whatever data is excluded for PIPEDA purposes is excluded from this definition.

3. OUR COMMITMENT TO PRIVACY

Scelta employs state-of-the-art security measures to protect your data, including encryption, secure cloud storage, and regular security assessments. Our commitment to data security is at the forefront of our operations, ensuring your information is protected against identity theft and unauthorized access or disclosure to the greatest extent reasonably possible.

At Scelta, we are dedicated to safeguarding your personal information and upholding the standards set forth by the Personal Information Protection and Electronic Documents Act (PIPEDA). Our Privacy Policy is designed to be clear, concise, and understandable, ensuring you are fully informed about how we manage your personal information.

Scelta is deeply committed to protecting the privacy and security of all client data entrusted to us. This commitment is a cornerstone of our services and operations. Our practices for collecting, using, and protecting your personal and business information are detailed comprehensively in this Privacy Policy. We adhere to industry-standard security measures to prevent unauthorized access, alteration, disclosure, or destruction of your data.

4. PRINCIPLES OF OUR PRIVACY POLICY

Scelta's principles are based on PIPEDA's principles. They are grounded in the concept that any collection, use or disclosure of personal information must only be for purposes that a reasonable person would consider appropriate in the circumstances

Principle 1 – Accountability: Scelta is responsible for personal information under its control. It ensures that at all times someone is appointed to be accountable for its compliance with these fair information principles.

Principle 2 - Identifying Purposes: The purposes for which the personal information is being collected will be identified by the Scelta before or at the time of collection.

Principle 3 – Consent: The knowledge and consent of individuals are required for the collection, use, or disclosure of personal information, except where inappropriate. Scelta reasonably relies on its clients to ensure that its employees, users and other individuals init its organizations have been informed of their rights and freely and voluntarily consent to their personal information being used in the Scelta service.

Principle 4 - Limiting Collection: The collection of personal information is limited to that which is needed for the purposes supplying Scelta's service. This information is collected by fair and lawful means.

Principle 5 - Limiting Use, Disclosure, and Retention: Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information will only be kept as long as required to serve those purposes.

Principle 6 – Accuracy: Personal information will as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.

Principle 7 – Safeguards: Personal information will be protected by appropriate security relative to the sensitivity of the information.

Principle 8 – Openness: Scelta is making detailed information about its policies and practices relating to managing personal information publicly and readily available through this Privacy Policy.

Principle 9 - Individual Access: Upon request, an individual will be informed of the existence, use, and disclosure of their personal information and be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10 - Challenging Compliance: An individual shall be able to challenge Scelta's compliance with the above principles. Their challenge should be addressed to the person accountable for the organization's compliance with PIPEDA or directly to PIPEDA if they are unsatisfied with the response.

5. GOOGLE CALENDAR INTEGRATION AND DATA USAGE POLICY

Our Portal application accesses Google Calendar data, specifically through the **Google Calendar Events API**. We adhere to strict data access, usage, retention, and security policies to protect user privacy

1. What Google user data is accessed by our application?

We only request permission to access, create, edit, and delete calendar events created by our app. We do **not** access, view, or modify any other events on the user's calendar that were not created through our application.

2. How does our application use Google user data?

We use Google Calendar data solely to provide our users with event management functionality within our application. This includes:

- Creating new calendar events on behalf of the user when an event is scheduled using our application, either by the user or by team members/admins on their behalf.

- Updating events that were created by our application in case the user needs to modify event details.
- Deleting events created by our application if the user chooses to remove them. We do **not** use Google user data for any other purposes, such as analytics, advertising, or sharing with third parties.

3. With whom do we share, transfer, or disclose Google user data?

We **do not** share, sell, transfer, or disclose Google user data to any third parties. The only interaction with user data is between our application and Google Calendar, strictly for the intended purpose of managing user events.

4. What are our policies around the retention or deletion of Google user data?

Our application does not store or retain Google Calendar event data beyond what is necessary for event management. Any event created, modified, or deleted through our application is directly updated in the user's Google Calendar. If a user deletes an event through our app, it is immediately removed from Google Calendar. We do not keep any copies of event data on our servers. Additionally, if a user revokes our app's access to their Google Calendar, we no longer have any ability to access or manage their events.

6. MICROSOFT OUTLOOK CALENDAR INTEGRATION AND DATA USAGE POLICY

Our Portal application accesses Microsoft Outlook Calendar data specifically through the **Microsoft Outlook Calendar Events API**. We adhere to strict data access, usage, retention, and security policies to protect user privacy

1. What Microsoft Outlook user data is accessed by our application?

We only request permission to access, create, edit, and delete calendar events created by our app. We do **not** access, view, or modify any other events on the user's calendar that were not created through our application.

2. How does our application use Microsoft Outlook user data?

We use Microsoft Outlook Calendar data solely to provide our users with event management functionality within our application. This includes:

- Creating new calendar events on behalf of the user when an event is scheduled using our application, either by the user or by team members/admins on their behalf.
- Updating events that were created by our application in case the user needs to modify event details.
- Deleting events created by our application if the user chooses to remove them. We do **not** use Microsoft Outlook user data for any other purposes, such as analytics, advertising, or sharing with third parties.

3. With whom do we share, transfer, or disclose Microsoft Outlook user data?

We **do not** share, sell, transfer, or disclose Microsoft Outlook user data to any third parties. The only interaction with user data is between our application and Microsoft Outlook Calendar, strictly for the intended purpose of managing user events.

4. What are our policies around the retention or deletion of Microsoft Outlook user data?

Our application does not store or retain Microsoft Outlook Calendar event data beyond what is necessary for event management. Any event created, modified, or deleted through our application is directly updated in the user's Microsoft Outlook Calendar. If a user deletes an event through our app, it is immediately removed from Microsoft Outlook Calendar. We do not keep any copies of event data on our servers. Additionally, if a user revokes our app's access to their Microsoft Outlook Calendar, we no longer have any ability to access or manage their events.

7. ADDITIONAL NOTIFICATIONS

Subprocessors: Subprocessors perform various functions related to our services, such as informant hosting, data analysis, and integration services. Your information may be shared with the subprocessors listed in the Appendix at the bottom of this Privacy Policy, who assist in providing the service. These entities are subject to strict data processing terms that protect your information. By using Scelta's services, you consent to sharing your information with subprocessors as necessary to provide and improve our services.

Modifications to Terms: Scelta reserves the right, at its discretion, to modify or replace these terms at any time. If a revision is material, we will provide at least 30 days' notice prior to any new terms taking effect. By continuing to access or use our services after those revisions become effective, you agree to be bound by the revised terms.

Effective Date and Version Information: This Privacy Policy is effective as of March 1st, 2025. It will remain in effect except concerning any changes in its provisions in the future, which will be in effect immediately after being posted on this page. If you have any questions or concerns about this Privacy Policy or Scelta's data practices, please get in touch with us.

APPENDIX - SUBPROCESSOR LIST

NAME	PURPOSE	LOCATION
Google Search	Research	Google Cloud
Google Calendar	Information Processing	Google Cloud
Google Sheets	Information Processing	Google Cloud
Google Forms	Information Processing	Google Cloud
Google AppSheet	Information Processing	Google Cloud
Goggle Docs	Information Processing	Google Cloud
Google Drive	Information Processing	Google Cloud
Microsoft Outlook	Information Processing	OneDrive
Calendly	Information Processing	Google
Digital Ocean	Information Processing	Digital Ocean Cloud

PipeDrive	CRM	Google
QuickBooks	Information Processing	Google
Stripe	Direct Debit Service	Google
Microsoft Office 365	Information Processing	Google, Bing
Microsoft Azure	Information Processing	Google, Bing
Wix	Website Services	Google
Canva	Website Services	Google
GitHub	Development	Github Cloud
OpenAi	Research	Google, Bing
Adobe	Information Processing	Google, Bing