inWebo Privacy Policy

November 20th, 2018
Prior Versions: January 15th, 2018
See this document online here

What We Collect

inWebo Websites

The inWebo corporate websites (www.inwebo.com, de.inwebo.com, www.inwebo.fr), as well as inWebo developer website (developer.inwebo.com), together "inWebo Websites" are managed by In-Webo Technologies ("inWebo"), a French registered corporation.

When you fill out a form on the inWebo Websites, we will create a record in our systems including information such as your name, email address, company, role, and phone number. We use this information for marketing and prospecting purposes.

As a visitor to inWebo Websites, you can ask us whether we have a profile and information (such as forms filled out and our pages visited) about you and, if so, to view, correct, or delete it, or to request us to not receive marketing or prospecting communications from us. For this, please write to privacy (at) inwebo (dot) com and provide your email address so we can search for what information we might have tied to that email address. Please note that for most visitors, we don't have any such information. Additionally, any marketing communication you receive from us contains a link to unsubscribe. Please also note that you have the right to file a complaint regarding these data with a Controlling Authority introduced by the EU General Data Protection Regulation (GDPR).

We contract with third-party service providers to host inWebo Websites and to provide other services to us related to these websites, such as helping us automate our marketing interactions. We require our service providers to agree not to access or use any information or data they may have access to while providing services to inWebo other than as specified by us.

None of the data we might collect about visitors of inWebo Websites is sold or even shared with any third party.

inWebo authentication solutions

inWebo provides organizations such as companies, banks, and healthcare providers with a solution that they use to more securely authenticate their users – such as employees, contractors, customers – accessing their online applications. To understand how these organizations you have a relationship with use your data, you should review their privacy policies.

If one of our customers (an organization) provides you with an inWebo authentication method to sign in to its applications, we will have a record in our systems that might contain data such as your username with that organization, your first and last name, and your email address. The data we have depends on how that organization uses our solution since we do not need any of these data to operate our service.

Also, when you are using our solutions, you might be given the possibility to name your profiles and devices, for the sole purpose of making it easier for you to recognize and distinguish them. Unlike authentication data that we protect with the highest grade of security measures and equipment, these names are not considered as sensitive data in our systems

and therefore do not benefit from the extra security measures used to protect sensitive data. This is therefore your responsibility to make sure that the names you are using are not sensitive data and that you would not suffer any damage in the event that this data was accidentally made available to a non-authorized party. In plain English: for the purpose of naming your profiles or devices, never use information such as your SSN, a tax ID, a driver's license number, a credit card number, or a password. Use nicknames instead such as "July Home", "Mary Work", "John private", etc.

We have a commitment to our customers to not access or alter the information they use to authenticate their users and to protect their applications, or the information that is collected for this purpose. We do not process or share it with any third party. We have a strict internal policy to not access it without a specific request from the organization that created it and then for the sole purpose of analyzing or solving an issue impacting the authentication service for that organization.

We record information about how the authentication solution is used to access our customers' applications. We therefore store in our systems data such as day and time of access and sometimes IP address, authentication method used, and authentication result. We do not process or share this information with anyone but the organization using our solution to authenticate their users.

Since the data in our systems is primarily created by our customers using their identifiers of their users (like usernames and anonymous aliases), in most cases, we are unable to know whether we have data about you as a user of our customers' applications. Any requests to view, correct, or delete personal data, or any question or complaint you might have with the use of that data must be made to the organization that created an authentication profile for you in our systems. If you have made a request to delete your profile in our systems but are unsure whether the organization has executed it, you might go on this web page and enter your email address with that organization in the "returning user" section. If this address still exists in our systems, you will receive an automated email listing which organization(s) still hold(s) data about you in our systems.

No Tracking of Your Browsing

inWebo Websites

We use Google Analytics code and some similar tools on the inWebo Websites to obtain browsing statistics with the purpose of making the website more relevant for our visitors. Browsing statistics are aggregate data (such as number of page views, sessions, percentage of new visitors vs. returning users) that do not provide inWebo with any personal data such as your name, IP address, device identifier, or email address. Please see Google Analytics' privacy policy for current details on Google's practices.

We also use Google Analytics for retargeting ads (which means showing ads on Google's Display Ad Network to people who previously visited certain pages of the inWebo Websites). As a visitor to the inWebo Websites, you can avoid being added to a Google Analytics retargeting list by installing a browser add-on here. We respect your choice, and it will not alter your browsing experience on our websites.

inWebo does not collect data about your browsing behavior beyond our websites.

inWebo authentication solutions

There is no tracking of your browsing implemented in our authentication solutions.

Security

inWebo Websites

We implement SSL certificates on inWebo Websites so that you can have the guaranty, while browsing on them, that you are on a trusted and legitimate website. We also use these certificates to encrypt (https) the information you enter on inWebo Websites by filling out a form. The information you provide and the data that might be gathered from further interactions with inWebo Websites is stored under our direction by our Marketing Automation and Customer Relationship Management service providers that have stated in their privacy policies that they have put in place suitable physical, electronic and managerial procedures to safeguard and secure this information.

inWebo authentication solution

If an organization has created an authentication profile for you in our systems, we have policies to use appropriate physical, electronic, and managerial procedures to safeguard and secure it. These policies include hosting our systems in ISO27001-certified data centers and using firewalls, encryption, and certified hardware security appliances.

What Data Is Sent Outside the EU and Where

Currently, inWebo does not transfer data gathered within the EU to locales outside the EU.

Government Requests

Notwithstanding anything to the contrary in this policy, we may preserve or disclose your information if we believe that it is reasonably necessary to comply with a law, regulation, or legal request or to protect the safety, property, or rights of inWebo or others. However, nothing in this policy is intended to limit any legal defenses or objections that you may have to a third party or government request to disclose your information.

Data Retention

Given the retention requirements of some regulatory bodies and similar requirements of the customers that create user profiles in our systems, we have a policy in place to delete authentication usage data six months after that data was created in our systems. As an exception, we will store authentication usage data during a longer period of time if a customer has an archiving contract with us that requires a longer retention of their users' authentication usage data. Given the limited data we collect for the purpose of marketing and commercial prospecting, we do not have retention or deletion policies in place for that data.

Change of Control

If inWebo is ever involved in a bankruptcy, merger, acquisition, reorganization, or sale of assets, your information may be sold or transferred as part of that transaction. The promises in this policy will apply to your information as transferred to the new entity, including your right to delete your information entirely from our databases from use of the websites.

Changes and Contact Info

From time to time, we need to make changes to our Privacy Policy to account for new features or for other reasons. When such changes occur, you are able to track them on our websites as well as view the new document on our websites. By continuing to visit the websites or use our authentication solutions, you are consenting to the revised policy. If you have concerns about our policy, please forward them to privacy (at) inwebo (dot) com, and we'll try our best to respond promptly.