Policy Overview

If you have questions about alternatives for preserving your leads, please feel free to ask through our tickets.

We have rigorous data security measures. The system automatically scrubs sensitive field data from the system. In particular, the default security settings descriptions include that all sensitive and personally identifiable information (PII) fields are scheduled to automatically delete from your boberdoo system after 30 days.

Thirty days is the maximum. If you need to retain data, we recommend setting up timed reports so you can export the leads before they reach that limit. Weekly timed reports, for example, may work for you. We can shorten this deletion timer or securely export fields to your Amazon S3 account before deletion.

Please refer to the links below to learn more about the security settings and recommendations for preserving your leads.
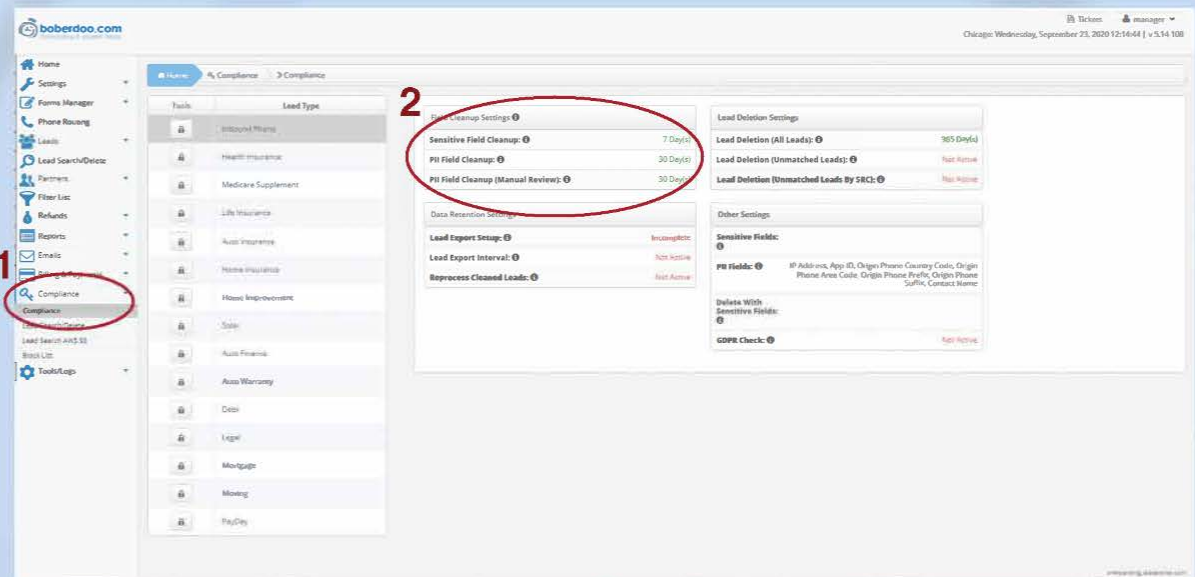
- Security
- Default Security Settings
- Data Retention

Step 1

Select the Compliance tab.

Step 2

Review current restrictions.

Related Links

Main Page

Video

Support Page

Compliance

Policy Overview

If you have questions about alternatives for preserving your leads, please feel free to ask through our tickets.

If you log into your system and click on the Compliance page, you will see exact details of which fields are marked as PII and which are marked as Sensitive/Delete with Sensitive. In general, PII is name, address, email, phone and IP address.
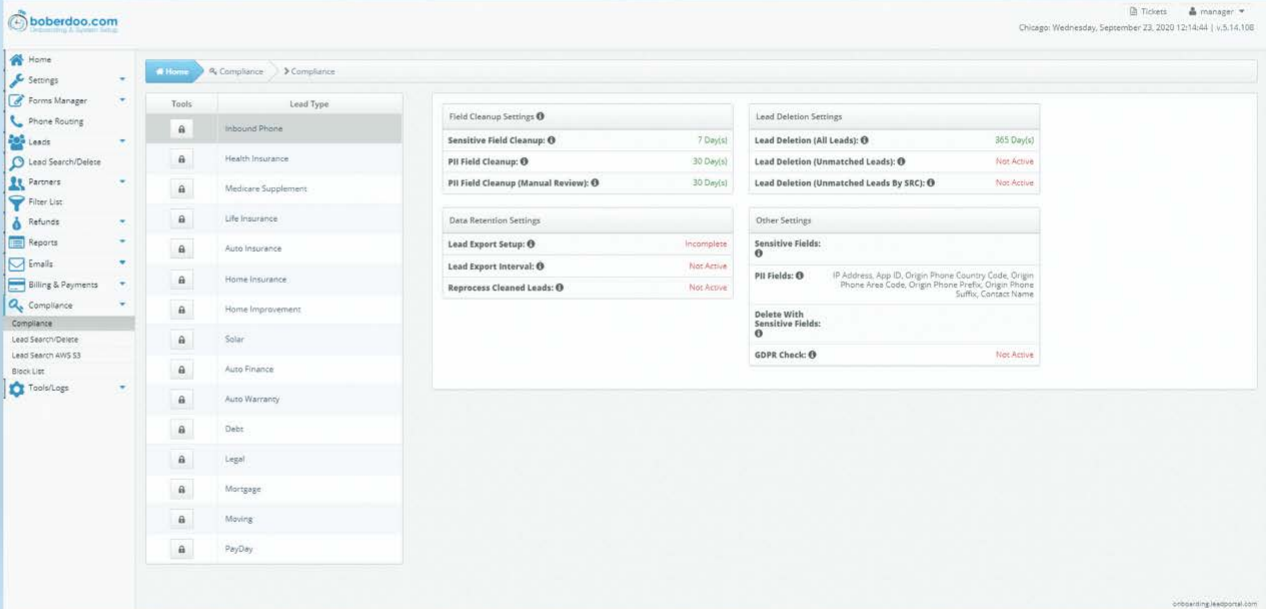
Those get cleared at 30 days. Sensitive is personal health information, financial information, account numbers and date of birth. Those get cleared at 7 days. The email address will be in boberdoo for 30 days.

Also, when we clear the email and phone, we store a hashed value in boberdoo so you can still search for an email address, and we can find the lead(s) based on that hashed email after the 30 days.

Related Links
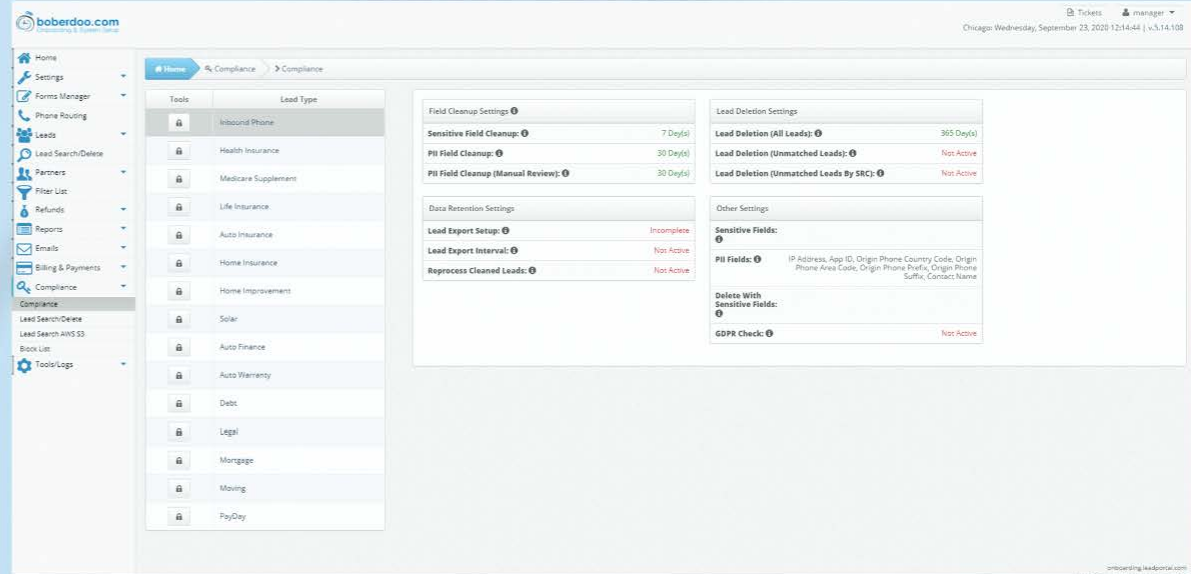
Main Page

Video

Support Page

Policy Overview

If you have questions about alternatives for preserving your leads, please feel free to ask through our tickets.

boberdoo has implemented a 7-day sensitive field and 90-day PII field cleanup process for your lead system. Our process automatically exports your data to Amazon S3 and has tools to do things like research leads by email or phone and reprocessing options even after this data is removed from your lead system.

As it currently stands, we have the data going into a S3 account but need to transfer ownership if you want to retain the account. This would be an account in your company's name, and you would pay Amazon directly for the usage.

Here are some good resources with more information:

 - Compliance
 - Lead Field Security

Currently, clients are paying $20/month or less. If you want us to transfer ownership of this AWS S3 account, we will need the following information **ASAP**:

Company Name (including any LLC, Corp, etc.)
Contact Person Full Name
Contact Person Email (with company email address if possible)

Related Links

Main Page

Video

Support Page