Product Privacy Statement

Effective as of July 5 2025.

Vault Platform, Inc. and its affiliates (collectively, “Vault Platform”, “we”, “us”, or “our”) provide a solution for misconduct reporting for workplace personnel.

Table of Contents:

Overview

This “Product Privacy Statement” explains how we collect, use, disclose or otherwise process the personal data of employees, contractors or other personnel of (a) our business customers who engage us to provide the Services (as defined below) to them (each a “Business Customer”) and (b) our Business Customers’ vendors, customers or other stakeholders (each such employee, contractor or other personnel, an “End User”) on behalf of our Business Customers in connection with our products and services, including the Vault Platform all in one integrity platform, mobile application, browser-based application or other intake methods and browser-based online case management application (collectively, the “Services”).

If you are an End User using our Services on behalf of, or as allowed by, one of our Business Customers, Vault Platform is the data processor and the Business Customer is the data controller with respect to your personal data. In most cases, the Business Customer will be your employer.

Because the Business Customer is the data controller, it is primarily the Business Customer that is responsible for how your personal data is collected, processed and shared in accordance with data protection laws. Therefore, if you have questions or concerns about the processing of your personal data, you should contact the Business Customer directly or refer to its separate privacy policies.

Vault Platform's processing of your personal data in connection with the Services is governed by this Product Privacy Statement and the contractual arrangement with the Business Customer. In the event of any conflict between this Product Privacy Statement and the agreement with the Business Customer, the Business Customer's agreement will control to the extent permitted by applicable law.

This Product Privacy Statement is not a substitute for any privacy notice that the Business Customers are required to provide to End Users.

Personal Data We Collect on The Business Customer's Behalf

The type of personal data that Vault Platform may collect on the Business Customer's behalf and the timing of when it may be shared with the Business Customer is explained in this section.

In using the Services, you may provide certain personal data about yourself and other End Users if you decide, at your discretion, to report an incident or other misconduct committed by another End User (the "Named Offender"). We **do not share with the Business Customer any of the personal data you have inputted to the Vault Platform about yourself or other End Users (including the Named Offender) unless and until you instruct us to do so,** by **submitting** your misconduct report through one of the reporting options via the Services. Your name will not be notified to the Business Customer if you decide to submit the report anonymously, but we will provide the Business Customer with any content

you choose to disclose when submitting the report, which may include personal data about yourself – **please note that any such personal data may enable the Business Customer to determine or infer your identity**. As also described in the "Personal data you provide to us" section below, any content you choose to provide is entirely at your discretion.

When using the "**GoTogether®**" functionality to report an incident or other misconduct committed by a Named Offender, you provide personal data about yourself and personal data about the Named Offender. The report, and any associated personal data about yourself and the Named Offender, are not submitted to the Business Customer until and unless another report is or was submitted by another End User to report an incident or other misconduct committed by the same Named Offender, and only then your report will be submitted to the Business Customer and your report status will be classified as "New".

We may also collect, on behalf of the Business Customer, and share with the Business Customer, personal data about you that is provided to us by other End Users when submitting a misconduct report using the Services.

Personal data you provide to us.

The personal data you provide to us through the Services (and which we collect on behalf of the Business Customer) may include:

- **Business and personal contact information,** such as your first and last name, email address, your relationship with the Business Customer, role, department, work site and location, the electronic identifying number allocated to you by the Business Customer, and the Business Customer's name.
- **Content you choose to upload to the Services,** such as text, including text messaging, images, audio, and video, along with the metadata associated with the files you upload and any other personal data you choose to provide when you use any interactive features of the Services. Any content you choose to provide is entirely at your discretion.
- **Profile information,** such as your username and password that you may set to establish an online account for the Services.
- **Feedback or correspondence,** such as personal data you provide when you contact us with questions, feedback, or otherwise correspond with us online.

- **Other personal data** that we may collect which is not specifically listed here, but which we will use in accordance with this Product Privacy Statement, the Business Customer's instructions, or as otherwise disclosed at the time of collection. Such personal data may include work history, skills and experience.

Personal data we obtain from the Business Customer or other End Users.

As explained above, we may collect personal data about you which is provided by the Business Customer or other End Users. For example, your co-workers or the Business Customer may share its messages, files or other content in reporting and/or in connection to case management, investigating and analyzing reports.

Cookies and other personal data collected by automated means

We and our service providers may automatically log information about you, your computer or mobile device and activity occurring on or through the Services – for the purpose of Service enablement and improvement. The information that may be collected automatically includes your IP address, computer or mobile device operating system type and version number, manufacturer and model, device identifier, default language, browser type, screen resolution, general location information such as city, state or general geographic area (not precise location), metadata; and information about your use of and actions on the Services and how you interact with us, such as pages or screens you viewed, how long you spent on a page or screen, navigation paths between pages or screens, information about your activity on a page or screen, access times, and length of access.

We and our service providers may collect this information directly or through our use of third-party software development kits ("SDKs"). We are using Sentry and Intercom SDKs.

How We Use your Personal Data

We use the personal data we collect at the instruction of the relevant Business Customer and in accordance with the agreement we have with the relevant Business Customer. As such, we may use your personal data to provide the

Services and for related internal purposes, including to:

- enable End Users to report workplace misconduct;
- improve the Business Customer and your Services;
- establish and maintain your user profile on the Services;
- communicate with you about the Services, including by sending you announcements, updates, new features, security alerts, and support and administrative messages;
- provide support and maintenance for the Services; and
- respond to your requests, questions and feedback.

In accordance with the agreement we have with the Business Customer, we may also use your personal data as we believe necessary or appropriate to (i) comply with any legal, regulatory, judicial, audit, or internal compliance requirements; and (ii) create anonymous or aggregate data from your personal data and the personal data of other End Users and use that personal data for our lawful business purposes.

How We Share your Personal Data

This section describes how Vault Platform may share and disclose your personal data. The Business Customer, as the data controller of your personal data, **determines its own policies and practices for the sharing and disclosure of your personal data.** Vault Platform does not control how they or any other third parties choose to share or disclose your personal data.

We do not share your personal data with third parties other than in accordance with the agreement with the Business Customer or if required to be disclosed by law, by any court of competent jurisdiction or by any regulatory or administrative body. We may share your personal data with the following entities and individuals as permitted by the Business Customer:

- Vault Platform's corporate affiliates and subsidiaries;
- Vault Platform's service providers that help or enable us to provide the Services (such as customer support, hosting, analytics, email delivery, and database management services). We ensure that our contracts with such service providers contain equivalent protections to personal data to those in

our contractual arrangements with the Business Customer.

We may also share your personal data with government, law enforcement officials or private parties as required by law, when we believe such disclosure is necessary or appropriate to (i) protect our rights, privacy, safety or property, and/or that of you or others; and (ii) protect, investigate and deter against fraudulent, harmful, unauthorized, unethical or illegal activity.

We may sell, transfer or otherwise share some or all of Vault Platform's business or assets, including the End Users' personal data, in connection with a business deal (or potential business deal) such as a merger, consolidation, acquisition, reorganization or sale of assets or in the event of bankruptcy.

Your Choices

As the Business Customer is the data controller in respect of the personal data that we hold about you and process as part of the Services, the Business Customer is primarily responsible for receiving and responding to your requests to exercise any rights afforded to you under applicable data protection laws, including in respect of the removal of your personal data ("Data Subject Requests"). We will cooperate with the Business Customer in respect of your Data Subject Requests in accordance with our contractual arrangements with the Business Customer.

Security Practices

Vault Platform takes security of your personal data very seriously. Vault Platform works hard to protect the personal data we hold about you and process as part of the Services from loss, misuse and unauthorized access or disclosure. These steps take into account the importance of the personal data we collect, process and store and the current state of technology. Vault Platform maintains compliance with various security frameworks such as ISO27001 and SOC2. [To learn more about Vault Platform's current practices and policies regarding security and confidentiality of the Services, please see our Security practices.]

App log-in
The Service uses biometric recognition traits (such as face or fingerprint) to establish your authentication and simplify accessibility. The biometric data is saved locally on your device and not collected or accessible by us.

Data Retention

Vault Platform retains your personal data for as long as necessary to (i) provide the Services; (ii) comply with regulatory, legal, audit or internal compliance requirements; and (iii) perform the terms of our contractual arrangements with the Business Customer.

International Data Transfers

Vault Platform is headquartered in the United States and hosted on Amazon Web Services (AWS) using data centres hosted exclusively in the United Kingdom. We have service providers in other countries and may transfer your personal data outside of the country in which you reside, including to the United States. Any transfer of your personal data will be carried out in accordance with our contractual arrangements with the Business Customer.

Changes to this Product Privacy Statement

We reserve the right to modify this Product Privacy Statement at any time. Similar to our Services, laws, regulations and industry standards may evolve, which may make changes to this Product Privacy Statement as necessary. We will post the changes to this page, to the Business Customer (data controller) or you and encourage you to review our Product Privacy Statement to stay informed. In accordance with applicable law, Vault Platform will provide additional notice, such as via email or through the Services, if necessary. If you disagree with the changes to this Product Privacy Statement, you should deactivate your Services account.

Any modifications to this Product Privacy Statement will be effective upon our posting the new terms and/or upon implementation of the new changes on the

Services (or as otherwise indicated at the time of posting). In all cases, your continued use of the Services after the posting of any modified Product Privacy Statement indicates your acceptance of the modified Product Privacy Statement.

How to Contact Us

Please direct any other questions or comments about this Product Privacy Statement or privacy practices to privacy@vaultplatform.com

For EU Residents: Please contact our EU Representative at Diligent Governance Ireland Limited, whose registered office is located at 6th Floor, South Bank House, Barrow Street, Dublin 4, Ireland.