Data Protection Statement for EthicsPoint Incident Management System

Data protection information on processing personal data related to the EthicsPoint Incident Management System (www.complianceactionline.ehticspoint.com)

Last updated June 2024

Fresenius Kabi AG ("we") will collect and use personal data of reporters using our Hotline and persons included in the reports.

This data protection statement informs you about the processing of personal data when filing or following up on a report in the EthicsPoint Incident Management System, available under **www.complianceactionline.ethicspoint.com** (hereinafter "Hotline Webportal"

Our Data Protection Policy

We have adopted Binding Corporate Rules on the protection of personal data. These rules have been **approved** by the European Data Protection Authorities and describe the principles for protecting personal data and determine how we apply them when collecting and using personal data.

The **Fresenius Binding Corporate Rules**, associated security policies and procedures aim to create a global adequate and uniform level of data protection across our group. They set the rules for the internal data transfers between Fresenius Kabi companies and our internal service providers worldwide.

Our Security Measures

We know information security is important to our customers, patients, and business partners. We are committed to maintaining information security through responsible management, appropriate use, and protection of our and your data in accordance with legal and regulatory requirements and our agreements. Please find more about the **Information Security at Fresenius Kabi**.

Why We Collect and Use Your Data

We collect and use your data for the following purposes:

- Performing assessments, investigations and remediation steps based on the incident reported
- Communicating with Reporters by sending follow-ups and conversations related to the reports and respond to questions and requests
- Authorizing reporters access to a report filed
- Preventing and detecting misuse and malfunction of the Hotline Webportal including troubleshooting
- Providing the Hotline Webportal and its functionalities
- Improving the Hotline Webportal's features and functionalities

What Data We Collect and How We Do That

We may collect and use your personal data in the following situation:

Information reporters provide to us

Reporters are not required to provide any personal data when filing a report in the Hotline Webportal. They can file a report entirely anonymously.

Should reporters decide to file a report in the Hotline Webportal or via direct email to compliance@fresenius-kabi.com and provide contact details or any other personal data, we will process the information they decide to submit. Such data particularly may include the following data:

- First and last name
- Country of residence
- Contact details, including email or telephone number
- Details related to the relationship with Fresenius Kabi and/or employees of Fresenius Kabi relevant to enable Fresenius Kabi to understand the context of your report
- Personal details related to the nature of the incident reported
- Name of individuals involved in the incident reported
- Date of the incident reported
- Name of the Fresenius company the report is related to
- Category of incident reported
- Details indicating how you learnt of the incident (Source)

- Details provided in any follow-up conversations through the Webportal
- Details included in any documents uploaded to the Webportal and comments made in the Webportal
- Password generated for any follow-ups

When visiting the Hotline Webportal

We collect data of a reporter's visit to our Hotline Webportal. We do this to present the website optimized to the device they are using and with all its functions or to store their preferences for their current or future browsing sessions.

We collect the following internet protocol data during visits on our websites:

- the name of a visitor's service provider including IP address. Visitors' IP address will be used in a pseudonymized manner by deleting the last three digits. That way we are no longer able to directly identify them as an individual.
- the website that directed them to our site
- the pages visited on our website
- their web browser type, and
- the date and length of their visit.

Information we collect by using cookies

We use cookies on our website. Cookies are small text files that are stored locally on a visitor's computer by your web browser.

We use the following types of cookies:

Strictly necessary cookies

This type of cookies is required to make the website work. They are exclusively used by us during the session and are therefore so called first party session cookies.

They help to make the page load more quickly and to limit the number of sessions originating from a user to prevent a website-overload.

They remain valid during the session and are automatically deleted when you close the browser.

Legal Basis for Processing Your Data

We process your personal data on one or more of the following legal basis:

- The processing is necessary for purposes of the legitimate interests pursued by us or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (Art. 6 (1) f) GDPR). This legitimate interest is explained under 'Why we collect and use your data'
- The processing of your personal data is necessary for us in order to comply with a legal obligation we are subject to (Art. 6.1 c GDPR). To fulfill obligations as generally stated in the (German) Criminal Code (re theft, embezzlement, Sexual harassment, Fraud, cyber fraud) and as mentioned e.g., in the AML § 10 and further in the Act against the restrains of competition (Cartel Act); US Sentencing Guidelines and (upcoming) EU Whistleblower Directive, require organizations to have a whistleblowing guideline as part of a compliance program.
- The processing of your personal data is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller such as the responsibility of board members to which Fresenius Kabi is bound.
- The processing of your personal data is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity, which potentially arising from reported compliance cases.
- The processing of your personal data is necessary for the purpose of the employment relationship on the basis of an employment agreement, Art. 88 GDPR in conjunction with national flexibility clauses of an EU-Member state (e.g. § 26 Federal Data Protection Act in Germany)

We Share Your Data

We collaborate with other organizations to achieve our purposes. Therefore, in compliance with our strict rules of confidentiality, we may send your personal data in parts or as a whole to other organizations.

Apart from the specific recipients as mentioned above for the specific situations, such recipients are:

- Other **Fresenius Kabi Group companies**
- Other **Fresenius Group Companies**
- Auditors, law firms and other consultants providing services to Fresenius Kabi
- Authorities, courts, parties in a litigation to the extent required to:

    - Meet any applicable law, regulation, legal process or enforceable governmental request
    - Enforce applicable Terms of Service, including investigation of potential violations
    - Detect, prevent or otherwise address fraud, security or technical issues
    - Protect against harm to the rights, property or safety of Fresenius Kabi or the users as required or permitted by law
- Data processors that process the data on our behalf and are bound by instructions. The data processor may be able to:
    - View statistics regarding your report
    - Alter your web portal password on request
    - Disable or terminate your access. Receive your submission related information in order to satisfy applicable law, regulation, legal process or enforceable governmental request.
    - Restrict your ability to delete or edit information or privacy settings.

International Data Transfers

We may send your personal data in parts or as a whole to the above recipients in other countries. For some of these countries the European Commission or respective legislator or authority in your country has determined an adequate level of data protection to be in place that matches the level of data protection in your country.

The European Commission has done this for the following countries / international organizations in which Fresenius entities are located: Argentina, Canada, Japan, South-Korea, United Kingdom, New Zealand, Switzerland or Uruguay.

For countries where the respective legislator or authority has not decided that an adequate level of data protection exists that matches the level of data protection in your country, we have provided safeguards in order to secure your personal data to a degree that is equivalent to the level of data protection in the European Union or your home country as a minimum.

These safeguards are:

- For the exchange of data within our company: our Binding Corporate Rules for Controllers
- For the exchange of data with our service providers and other international organizations: Standard Contractual Clauses that have been issued by the European Commission, and/or as issued by other authorities or legislators as applicable.

How Long We Retain Your Data

Generally, we store your personal data for one of the following periods of time:

- As long as we have a duty to retain the data in line with applicable laws (e.g., because we are obliged to store the data for tax purposes)
- If there is no legal retention applicable, at least for the term of the contractual relationship with you or the company you are working for
- If we have a legitimate interest, as laid down above, to process your personal data outside of such a contractual relationship, we process it for as long as we still have a legitimate interest in processing this data. The exact period depends on the company you are working for and your position in the company

If the legal retention period is longer than for the other above-mentioned ones, we aim to block the data until the end of the respective retention period and then erase it.

Requests, Inquiries and Complaints

Depending on the situation you have certain rights regarding your personal data. You have the right to:

- Request access to your personal data
- Request rectification of your personal data
- Request erasure of your personal data
- Request the restriction of processing of your personal data
- Data portability
- Object on grounds specific to your situation

In these cases, please use our online **data protection contact form.**

You also have the right to lodge a complaint with our data protection officer or the supervisory authority.

Data Protection Officer:

Fresenius Kabi AG
Data Protection Officer
Else-Kröner-Straße 1
61352 Bad Homburg
Germany
E-mail: **dataprotectionofficer@fresenius-kabi.com**

Data Protection Authority:

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit
Presse- und Öffentlichkeitsarbeit
Gustav-Stresemann-Ring 1
65189 Wiesbaden

Further Information for Specific Situations

Changes to this data protection statement

As the collection and use of your data may change over time, we might also modify this data protection statement to always correctly reflect our data processing practices. We encourage you to review it from time to time.

Controller and Contact

The controller and responsible entity for processing of personal data is:

Fresenius Kabi AG
Else-Kröner-Straße 1
61352 Bad Homburg
Germany
Contact