The processing of personal data is subject to the EU General Data Protection Regulation (GDPR).
This data protection notice informs you about how Fresenius SE & Co. KGaA Fresenius Digital Technology GmbH ("we" or "Fresenius") process personal data of you as a data subject ("you") in the context of compliance case management and what kind of data is involved.
In accordance with the Telecommunications Digital Services Data Protection Act (TDDDG), this data protection notice also informs you about how your personal data and information is processed in your terminal equipment (e.g. laptop or smartphone), when using the whistleblower portal (website freseniusgroup.ethicspoint.com, freseniusgroupmobile.ethicspoint.com) and what data is involved.
"Personal data" means all information about you as data subject.
"Processing" means any operation performed upon personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
With this data protection information, we explain to you in detail, in particular:
- who is responsible for the processing of your personal data and whom you can contact if you have questions or wish to make a complaint (Section 1);
- how we collect your data, what data we collect and for what purposes we process these personal data, on which legal bases we rely on in this regard and how long we store your personal data (Section 2);
- to whom we may transfer your personal data (Sections 3);
- how you can update, correct or delete your personal data and exercise other rights in relation to your personal data (Section 4) and
- in which other situations your personal data may be processed and how you can contact us (Section 5).

1. Controller and contact details

The controller responsible for the processing of your personal data is for data subjects who have concluded a work contract with one of the following companies or are in contract negotiations:
- Fresenius SE & Co. KGaA, Else-Kröner-Straße 1, 61352 Bad Homburg or
- Fresenius Digital Technology GmbH, Else-Kröner-Str. 1, 61352 Bad Homburg or

The controller responsible for the processing of your personal data is for all other data subjects:
Fresenius SE & Co. KGaA, Else-Kröner-Strasse 1, 61352 Bad Homburg, Germany
E-Mail: corporate-compliance@fresenius.com
According to the GDPR, we are obliged to provide you with the contact details of the data protection officer. You can contact the data protection officer by sending a letter to the postal address of the controller for the attention of the Data Protection Department or by e-mail via dataprotection@fresenius.com

2. Processing of personal data

2.1 General processing of your personal data in the context of an investigation (compliance case management)

We process personal data provided by you, provided by Fresenius itself, employees of Fresenius companies or third parties (depending on the circumstances, individuals and/or companies, defendants, participants or witnesses) or collected through the use of our systems or applications.

A compliance case management investigation is conducted specifically through fact-finding measures, which may include, but are not limited to: Interviews and collection of information; analysis of the roles and responsibilities of the data subjects; review of documents (e.g., contracts, invoices, evidence of services rendered, payment instructions); seizure and review of electronic data (e.g., analysis of data stored on the data subject's computer; analysis of e-mails; data from SAP or other IT systems that map or support business processes).

We process information that you, in particular, provide to us yourself and that is provided to us by other employees, other Fresenius companies or contractual partners in the course of an investigation, e.g. when you exchange e-mails with a contractual partner or work in a team with employees of your company or other Fresenius companies.
This personal data includes in particular:
- Name (e.g., first name, last name, birth name, title);
- Identification code (e.g. staff code, customer code);
- Address and contact data (e.g. street, street number, postal code, place of residence, country of residence, phone, email address);
- Personal information (e.g. date and place of birth, marital status, gender);
- Data on employment contracts (e.g. date of entry/exit, time limit, holiday, terms and conditions of employment, and terms and conditions of employment contracts, pension eligibility);
- Qualification (e.g. application documents, certificates, references, patent holder information, expert opinions or expertise);
- Organizational data (e.g. department, cost center, description of the position, title of the position (internal/external), management category, job code, occupational group and level, responsibilities and activities, company name and code of the employer, superior);
- Planning data (e.g., availability, service time, time needed for tasks);
- Government issued identifiers (e.g., social security number, tax number);
- Documents related to immigration laws and citizenship (e.g. national identification number, passport data, details of the residence permit or work permit) and necessary information, to extend or obtain a residence or work permit, as well as
- Social media profiles.

We process information that is collected in particular when you use or log in to one of our systems or applications.
This personal data includes in particular:
- IT application data (e.g. system identifiers, identifier for the single sign-on, system and device passwords), instant messaging accounts, video conferencing and other messaging accounts, network ID and infrastructure information, IP address, location information, workflow data (roles, activities), system and device logs, and electronic content generated by you using our enterprise systems and devices, as well as
- Information related to quality management processes (e.g., creation, modification of quality documents, date and time of performed test procedures).

All personal and special personal data may be processed for the above-mentioned purposes. For a list of the data, you can therefore refer to the data protection notice for employees or the data protection notice for business partners, visitors and recipients of public relations work published on the website www.fresenius.com.

A Compliance Case Management report can be made via website, hotline, e-mail, mail or in person. An anonymous report, as well as setting up a mailbox to conduct anonymous calls, can be made via website and hotline. When a report is made via the hotline, the voice recording is recorded and transmitted in writing.
The purpose of Compliance Case Management is to receive, investigate and respond to information about possible compliance violations at Fresenius. The processing is carried out in accordance with Fresenius' guidelines for compliance case management. The necessity of an investigation in the interest of the company is documented in an investigation order.
We process your personal data solely for the purpose of conducting our own review or investigation into this matter, obtaining appropriate insurance coverage, or for the purposes of securing and subsequently enforcing our claims relating to the subject matter of the investigation.

The authorisation to process personal data in the context of an employment relationship arises first of all from Art. 6 (1) (1) (b), from the necessity for the implementation or termination of the employment relationship, as well as Art. 9 (2) (1) (b) GDPR for the exercise of rights or the fulfillment of obligations under labor law and social security and social protection law.
For all data subject groups, there is also a legal obligation to operate an appropriate internal compliance management system pursuant to Art. 6 (1) (1) (c) GDPR, in conjunction with Section 12 (1) (1) HinSchG, Section 33 (1) WpHG, Section 91 (2) AktG, Section 43 (1) GmbHG, Art. 9 (2) (1) (f) GDPR and for certain employers to operate a whistleblower system pursuant to Art. 6 (1) (1) (c) GDPR, in conjunction with Sections 10, 12 (1) (1) HinSchG, Art. 9 (2) (1) (f) DS-GVO, § 10 (2) HinSchG as the basis for processing personal data.
The authorisation of the internal reporting office to pass on information about the identity of the whistleblower is based on your consent in accordance with Section 9 (3) HinSchG.

No later than three years after completion of the internal investigation, data processed exclusively within the framework of compliance case management will be deleted in accordance with legal requirements. Following the internal investigation, the data will be retained in the event of legal enforcement of claims or official proceedings for the duration of these proceedings and deleted upon their conclusion, unless the storage of the data is necessary for the preservation of evidence for the assertion, exercise or defense of legal claims within the scope of the statutory limitation provisions. According to Section 195 et seq. BGB, these limitation periods can be up to 30 years, with the regular limitation period being three years. In addition, further processing for a limited period may be necessary for the fulfillment of regulations, laws or other provisions of the European or national legislators.

2.2 Additional processing of your personal data based on the use of the whistleblower portal

2.2.1 Recording of technical characteristics when visiting the website

We collect information about your visit to our website, as we do with most other websites. When you visit our website, the web server temporarily records
- the domain name or IP address of your computer,
- the file request of the client (file name and URL),
- the http response code,
- the website from which you are visiting us,
- which Internet browser and which operating system you are using,
- the nature of your device,
- the date of your visit,
- as well as how long you've been here.

The logging of data is necessary for navigation through the pages and use of essential functions (section 25 (2) (2) TDDDG, Article 6 (1) (1) (b) GDPR). In addition, the data is used for the purpose of detecting and tracking abuse on the basis of the legitimate interests of data security and the functionality of the service (Article 6 (1) (1) (f) GDPR, section 25 (2) (2) TDDDG). In particular, no overriding interest of the data subject is opposed to a use for the defense against attempted attacks on our web server to ensure proper use.

The data will neither be used for the creation of individual profiles nor passed on to third parties and will be deleted after ninety days at the latest.

2.2.2 Usage of Cookies

When you visit a website, it may retrieve or store information about your browser. This usually takes the form of cookies and similar technologies. These are small text files that are stored locally on your device by your web browser. This can be information about you, your settings or your device. In most cases, the information is used to ensure that the website functions as expected. This information does not normally identify you directly. However, blocking certain types of cookies may result in a compromised experience with the website and services we provide.

We only use cookies that are absolutely necessary so that you can navigate through the pages and use essential functions. They enable basic functions, such as access to secure areas or setting your privacy preferences. The legal basis for these cookies is section 25 (2) (2) TDDDG, Article 6 (1) (1) (b) GDPR. If you block these cookies via your browser settings, some or all of these functions may not work properly.

Navex.com	ASPSESSIONID*, ep, N1Secure_Incidents,	First Party	Browser Session
Navex.com	incap_ses_*, nlbi_*, reese84, x-d-token, __utcmv*	Second Party	Browser Session

The aforementioned cookies are automatically deleted when the browser session ends.

3. Possible recipients of personal data

In order to fulfill the aforementioned purposes, we may share your personal data in whole or in part with other group companies and/or service providers.
In addition, the following categories of recipients may receive your personal data:
- Authorities, courts, parties to a legal dispute or their designees to whom we are required to provide your personal data by applicable law, regulation, legal process or enforceable governmental order, e.g., law enforcement authorities, tax and customs authorities, regulatory authorities and their designees, financial market regulators, public registries;
- auditors or external consultants such as lawyers, tax advisors, insurers or banks, and
- another company in the event of a change of ownership, merger, acquisition or disposal of assets.

3.1 International data transfers

In order to fulfill the aforementioned purpose, we may transfer your personal data to recipients outside Germany. Transfers within the European Economic Area (EEA) always take place in accordance with the uniform EU data protection level.
Transfers to third countries are always carried out in compliance with the supplementary requirements of Article 44 et seq. GDPR.
Your personal data may be transferred to certain third countries for which an adequacy decision of the EU Commission determines that an adequate level of protection exists in accordance with the uniform EU level of data protection. The full list of these countries is available here (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions).
As a rule, EU standard contractual clauses ("SCC") are concluded with the recipient for transfers to other third countries. These have been issued by the EU Commission to safeguard such international data transfers.
To transfer personal data outside the EEA among group companies of the business segments Fresenius Kabi (Fresenius Kabi AG and its affiliated companies) and Fresenius Corporate, we implemented binding corporate rules ("BCR") approved by the data protection authorities in accordance with Article 47 GDPR. A copy of the SCC and the BCR can be requested via dataprotection@fresenius.com.
Ultimately, personal data may be transferred on the basis of an exceptional circumstance under Article 49 GDPR.

4. Your rights

According to the GDPR you are entitled to various rights. You have the right to access your personal data (Article 15 GDPR, section 34 et seq. BDSG), to correct incorrect personal data (Article 16 GDPR), to delete your personal data under certain circumstances (Article 17 GDPR, section 34 et seq. BDSG) and to restrict the processing of your personal data under certain circumstances (Article 18 GDPR).
Right to object on a case-by-case basis
In case the processing is based on Article 6 (1) (1) (e) or (f) GDPR including profiling based on those provisions, you have the right to object to the processing of your personal data on grounds relating to your particular situation (Article 21 (1) GDPR).
You also have the right to lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence, place of work or of an alleged infringement of the GDPR (Article 77 GDPR in conjunction with section 19 BDSG). The competent data protection authority for Fresenius SE & Co. KGaA and Fresenius Digital Technology GmbH is "Der Hessische Beauftragte für Datenschutz und Informationsfreiheit", Postfach 3163, 65021 Wiesbaden.
The right of appeal is without prejudice to any other administrative or judicial remedy.

5. further information on data processing in other contexts and our contact details

We may process your personal data in various other contexts, e.g. when you visit our website www.fresenius.com. For the processing of your personal data in these situations, please refer to the specific information in each case.
If you have any questions about data protection at Fresenius, please contact dataprotection@fresenius.com.