Data protection notice for business partners, visitors and recipients of public relations work

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 Netcare GmbH, Hyginus Publisher GmbH, Fresenius Versicherungsvermittlungs GmbH, Fresenius Management SE, Fresenius Immobilien-Verwaltungs-GmbH, Fresenius Immobilien-Verwaltungs-GmbH & Co. Friedberg KG, Fresenius Immobilien-Verwaltungs-GmbH & Co. Schweinfurt KG, Fresenius Immobilien-Verwaltungs-GmbH & Co. St. Wendel KG, (**"we"** or **"Fresenius"**) personal data of you as a business partner business partners, visitors and recipients of public relations work (**"you"**) and what data is involved.

By **"personal data"** we mean any information related to you.

By **"processing"** we mean any operation which is performed on personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

With this data protection notice, we explain to you in detail, among other things,

- who is responsible for processing your personal data, and who you can contact if you have questions or complaints (section 1)
- how we collect your data, what data we collect and for what purposes we process this personal data (sections 2.1 and 2.2)
- the legal basis on which we base this (section 2.3)
- to whom we may transfer your data (sections 3 and 4)
- how long we store your data (section 5)
- why we have a compelling need to know your personal data (section 6)
- how you can update, correct or even delete this data and exercise other rights in relation to your data (section 7) and
- give you further information for specific situations and contacts (section 8).

1. Controller and Contact

1.1 Responsible

The Fresenius company with which you have concluded a contract or are in the process of negotiating a contract and/or whose premises you visit and/or who is in contact with you in the context of public relations work is the data controller under the GDPR, as this company uses your personal data in the context of the respective relationship with you. The address and name of this Fresenius company can be found in the documents available to you.

1.2 Data protection officer

According to the GDPR, we are obliged to provide you with a data protection officer. This person can be contacted at the address of the responsible person for the attention of the data protection department or by e-mail: dataprotectionofficer@fresenius.com

2. Processing of personal data

2.1 How we collect your data and what data we process

We process personal data that you provide to us when you order our products and services, enter into a contract for the supply of goods and services with us, visit a premises or contact us in any way. In addition, personal data about you is collected when you log on to or use a system or application provided by us.

We also process personal data about you, your function in your company and as well as personal data of other executives and representatives, owners and shareholders of your company and the affiliated companies or your political mandate, which are published in predominantly publicly accessible commercial registers, websites, blogs and print media. This also includes other data sources that are publicly accessible or accessible to certain groups, in particular those made available by competent authorities and business associations.

We also process personal data relating to your company, you, other officers and agents, owners and shareholders of your company and affiliates, or your political mandate that is provided to us by service providers under contract, by other Fresenius companies or by competent authorities (including credit rating agencies, credit and risk information providers, financial services providers, governmental or international agencies or similar organizations, in particular tendering authorities or procurement authorities).

Such personal data may include your company name, your name, contact information, the names of your company's officers and agents and your company's affiliates, your company's bank accounts and payment information, the occupation and qualifications of your company's officers and agents, professional identifiers, organizational data, your company's affiliation data, certifications and quality statements, The information may include the bank account and payment information of your company, the occupation and qualifications of your company's officers and agents, professional identifiers, organizational data, affiliation data of your company, certifications and quality statements issued by your company's officers, agents or auditors, the names of your company's shareholders and your company's affiliates and the amount of ownership, information about public filings, trade registries and professional associations, as well as information about your company's disclosed transactions, including proposals and financing arrangements and past interactions with Fresenius and/or any of our affiliates.

Your personal data, such as names, email addresses, organisational details, may also be processed by us in connection with the use of Microsoft 365 Services. Microsoft 365 Services also creates internal analytics through aggregated reporting based on a use of your personal usage data. We also process your personal data in connection with the use of other company systems and devices. In particular, we process IT application data (e.g., system identifiers, single sign-on identifiers, system and device passwords), instant messaging, video conferencing and other messaging account data, network IDs and infrastructure information, geographic location information (such as GPS data, WI-FI access points, cell tower access points, IP addresses), workflow data (roles, activities), system and device logs, internet usage data (e.g. which web pages were visited and when), video recordings and content generated by you are processed. In addition, video and audio recordings made in connection with the use of MS Teams/ Skype and in the

context of operational video surveillance also contain contextual information on ethnic origin, religion or health.

2.2. Purposes of Processing

We process this data for the purpose of initiating, maintaining and/or terminating as well as assessing a (possible) business relationship with you. This general purpose includes in particular:

- the manufacture, provision and supply of products and services;
- the procurement of products and services from you;
- a potential investment in Fresenius shares, a potential acquisition, divestiture or joint venture transaction with us or an affiliate of Fresenius and/or an outside company;
- the exchange of information about existing contracts or possible contracts with you;
- the exchange/processing of business documents by means of the use of various Microsoft 365 Services. In principle, all Microsoft 365 services used have the overriding purpose of promoting communication and collaboration with external parties;
- create internal analytics for Fresenius' own use using Microsoft 365 services, such as MyAnalytics;
- the fulfilment of compliance requirements (e.g. conflict checks, business partner checks, sanctions list checks, money laundering identifications and controls, the verification of regulatory requirements for supply chains, customs and export requirements, traceability requirements for products);
- managing our relationship/communication with you or the company you work for (e.g. customer relationship management, supplier management, investor relations management);
- marketing (e.g. information about products and services or related information);
- assessing whether you are a suitable contact for specific business requirements, e.g. if we are looking for an expert in a particular area or for specific products;
- business partner assessment and qualification, e.g. whether you and your company meet certain quality and certification requirements;
- implementation and evaluation of the payment and accounting system, together with the collection of payments due to us, including the refinancing of receivables;
- assessing the financial solvency and credit risk of your company;
- organizing, securing and improving internal processes including communication, administration and IT (e.g. infrastructure and workplace management);
- organizing events for our company or if Fresenius provides the infrastructure for them (premises, IT infrastructure)
- crisis management for hazard prevention and response;
- in the area of communications management and information technology, the authorization of visitors for access to systems and applications and for access authorization/logging (authentication), e.g. when entering a building, a parking garage or a specific room, in particular by means of an access card or a key; location management, i.e. making room reservations, room management/planning; the use of the IT infrastructure and log-in data for the maintenance of the IT infrastructure in order to ensure IT support and for

troubleshooting; security management, i.e. making room reservations, room management/planning; the use of the IT infrastructure and log-in data for the maintenance of the IT infrastructure in order to ensure IT support and for troubleshooting; security management, i.e. making room reservations, room management/planning i.e. making room reservations, room management/planning; the use of the IT infrastructure and log-in data to maintain the IT infrastructure in order to ensure IT support and to identify and rectify errors; the security analysis, as well as the prevention of cyberattacks and the improvement of information security, including IT security.

2.3 Legal bases for processing

We process your personal data on one of the following legal bases:

- if the processing of your personal data is necessary for the performance of the contract concluded between you and us[1].
- if the processing of your personal data is necessary for us to comply with national and/or international legal obligations (e.g. employment laws, tax laws, social security laws, occupational health and safety laws, financial market laws, drug control laws, medical device laws, environmental laws, criminal and administrative offences laws, and commercial and corporate obligations), regulatory requirements (e.g. tax authorities, employment agencies, social security institutions) and public interests to which we are subject, and to provide evidence thereof[2].
- Since the processing is necessary for the purposes of the legitimate interests pursued by us or by a third party[3], unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child. These legitimate interests are:
    - fulfilling our contract with the company you work for, including enforcing any rights we have under that contract;
    - gathering information/knowledge management related to internal processes, products and services;
    - development, optimization and improvement of our products and services;
    - optimization of the administration;
    - conducting research;
    - organizational management;
    - risk management: hedging against e.g. financial/reputation risks;
    - internal Audit: performing internal audit procedures within the Group;
    - maintaining IT infrastructure, IT security, ensuring IT support, and identifying and resolving errors; and
    - compliance with and evidence of compliance with internal policies, national and international industry standards and legal obligations outside the EEA;
    - detection, investigation and prosecution of criminal offences and misdemeanours;

[1] Art. 6 I b) GDPR

[2] Art. 6 I c) or e) GDPR

[3] Art. 6 I f) GDPR

    - video surveillance and hazard prevention (especially building and facility security measures).
- If you have been informed about the intended processing of your personal data and have given us your consent[4]. You can revoke your consent at any time. You can withdraw your consent to the processing or for individual purposes of your choice. The withdrawal of consent does not affect the lawfulness of the processing based on your consent before the withdrawal. You can revoke your consent by sending an E-Mail to dataprotection@fresenius.com.

3. Possible recipients or categories of recipients of your personal data

In order to fulfil the above purposes, we may need to share some or all of your personal data with other companies. Recipients are:

- other group companies, if such transfer of personal data is necessary for the respective purpose;
- service providers who process personal data on our behalf but must follow our instructions for processing; these service providers are not permitted to use your personal data for purposes other than ours;
- authorities, courts, parties to a dispute or their designees to whom we are required to disclose your personal information pursuant to applicable law, regulation, legal process or enforceable governmental order, such as 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.

4. International Data Transfers

In order to fulfill the above-mentioned purposes, we may transfer your personal data to recipients outside Germany. For example, your personal data may be shared with other Fresenius Group companies in international projects in order to contact colleagues.

Your personal data may therefore be transferred internationally to countries in which the Fresenius Group operates. If your personal data is transferred to recipients within the European Economic Area, the data protection complies with European requirements.

If your data is transferred to recipients located outside the European Economic Area, we will ensure appropriate data protection. This data protection then also complies with the European data protection requirements. The transfer of personal data to recipients located outside the European Economic Area is carried out in compliance with the supplementary requirements of Art. 44 et seq. GDPR.

As a rule, corresponding contracts are concluded with these recipients, which include the EU standard contractual clauses (SCC) issued by the EU Commission to safeguard such international data transfers. The EU SCC used can be viewed here:

[4] Art. 6 I a) GDPR

- Clause Set I - Data transfers between controllers: https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:181:0019:0031:DE:PDF;
- Clause Set II - Data transfers between controllers: https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:DE:PDF;
- Clause Set III - Data transfers between controllers and processors: https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF.

Your personal data may also be transferred to recipients in countries for which the European Union has already decided that the European data protection requirements are complied with. As of today, these are, for example, Argentina, Canada, New Zealand, Switzerland and Uruguay. A complete list of countries with adequacy decisions can be found on the following page of the Hessian data protection authority: https://datenschutz.hessen.de/datenschutz/internationales/angemessenheitsbeschl%C3%BCsse.

Finally, personal data may be transferred on the basis of an exception under Art. 49 GDPR.

5. How long we store your personal data

As a rule, we store your personal data for one of the following periods:

- In accordance with applicable laws, for as long as we are subject to a retention obligation;
- Unless a mandatory record retention provision applies, we will retain your personal data for the duration of the contractual relationship with you or the company for which you work;
- In accordance with applicable law, as long as we have a legitimate interest outside of a contractual relationship;
- Preservation of evidence for the assertion, exercise or defence of legal claims within the framework of the statutory limitation provisions. According to §§ 195 ff. BGB, these limitation periods can be up to 30 years, with the regular limitation period being three years.

The exact period depends on the company you work for and your position in the company. In the case of longer retention periods (e.g. because we are obliged to store the data for the company audit), the aim is for the data to be blocked and archived until the end of the respective retention period and then deleted. Your data will be blocked for purposes other than archiving and kept until the end of the respective retention period.

6. Mandatory provision of personal data

You may need to provide us with your personal data to fulfil a contract with you or the company you work for. For example, we may need your contact details if you are our business contact with a supplier. If you do not provide your personal data, we may not be able to enter into the relevant contractual relationship.

7. Your rights

You have various rights under the GDPR. You have the right to access your personal data[5], to correct incorrect personal data[6], to delete your personal data under certain circumstances[7], to restrict the processing of the data under certain conditions[8] and the right to receive personal data provided to us in a structured, commonly used, machine-readable format for the purpose of transferring it to another business partner or organisation[9].

right to object on a case-by-case basis
According to Art. 21 I GDPR, data processing based on Art. 6 I e), f) GDPR, as well as profiling based on this provision, may be objected to for reasons arising from the particular situation of the data subject. The respective objection can be made form-free and is to be addressed to the controller.

You also have the right to lodge a complaint with a supervisory authority[10]. The data protection authority responsible for Fresenius 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.

8. Further information for special situations and contact persons

We may process your personal data in various other contexts, for example when you visit our website. 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.

[5] Art. 15 GDPR, §§ 34 ff. BDSG

[6] Art. 16 GDPR

[7] Art. 17 GDPR, §§ 34 BDSG

[8] Art. 18 GDPR

[9] Art. 20 GDPR

[10] Art. 77 GDPR in conjunction with § 19 BDSG