

PATIENT INFORMATION ON DATA PROTECTION

Dear patients¹,

As part of your treatment, care, or examination, it is necessary to process personal data and medical data (hereinafter referred to as “data”) about you. The protection of your data, openness, and transparency are important to us. Therefore, we are providing you with this patient information regarding the processing of your data and your rights under data protection law in accordance with Articles 15 through 22 of the EU General Data Protection Regulation (“GDPR”).

We perform various tasks, each of which requires the processing of your data. Processing takes place, on the one hand, as part of **medical consultations** in our practice and, on the other hand, during the **performance of laboratory analyses** in our own laboratory.

In the practice setting, data processing serves to initiate, establish, and carry out the treatment contract. If laboratory analyses are necessary as part of your treatment, we process your data additionally to initiate, establish, and carry out a so-called laboratory physician contract.

If a specific analysis cannot be performed in our own laboratory, we commission an external specialized laboratory and act as a so-called **“referrer.”** In this case, a direct laboratory contract is established between you and the commissioned laboratory. We represent you in this process to ensure the best possible medical care. In such cases, the commissioned laboratory is independently responsible under data protection law.

The collection and processing of health data is essential for your consultation, diagnosis, and treatment. Without the provision of the necessary information, comprehensive and careful medical care is not possible.

1. Who is responsible for processing your data?

The entity responsible for data processing is:

Institute of Immunology and Genetics GbR

Pfaffplatz 10, 67655 Kaiserslautern

Phone: +49(0)631-316700

2. Processing of your data in our practice, in our laboratory, or by a specialized laboratory commissioned by us

2.1 What categories of data are processed?

In the course of **practice and laboratory operations**, as well as when commissioning other **specialized laboratories (subcontracting)**, we process the following data from you in particular:

- **Patient master data and contact information**, e.g., title, first and last name, date of birth, address, phone number, email address, personal and marital status, and information regarding children, occupation, and nationality;
- **Data on authorized representatives, agents, or contact persons**, e.g., master and contact data, details regarding the nature of the representation and, if applicable, the degree of kinship;
- **Insurance data**, e.g., details regarding health insurance, insurance number, and other insurance information;

¹ For the sake of readability, we have omitted the use of all gender forms (m/f/d). All references to persons apply equally to all genders.

- **Laboratory and test results data**, e.g., laboratory analyses performed, test results, additional test results data, and information regarding the transmission of test results;
- **Sample and analysis data**, e.g., type, origin, and identification of the sample (e.g., barcode, sample ID).
- **Health data related to treatment**, e.g., medical histories, diagnoses, treatment recommendations, treatment courses, medication data, physician letters, referrals, treatment documentation, and other medical records;
- **Genetic data**, to the extent that such data is obtained in the course of genetic diagnostic testing;
- **Reporting data**, to the extent that reports are required by law (e.g., for findings subject to mandatory reporting);
- **Billing and payment data**, including information on creditworthiness and payment history.
- **Communication data**, e.g., information from correspondence with you as well as with co-treating physicians, medical laboratories, other medical facilities, or other third parties in connection with your treatment.

2.2 For what purposes is your data processed?

a) Medical Care and Treatment

- Processing of patient master and contact data as well as health data for medical care and treatment (preventive, diagnostic, therapeutic, curative, and follow-up).
- Counseling and informing patients about clinical pictures, treatment options, and risks.
- Use of digital and paper-based questionnaires to collect health data.
- Processing of special categories of data, e.g., regarding ethnic origin, genetic or biometric characteristics, to the extent medically necessary.
- Participation in interdisciplinary case conferences to analyze and coordinate diagnostics and therapy.
- Preparation of medical records such as physician letters and diagnostic reports for documentation and further treatment.

b) Billing, administration, and processing of treatment

- Billing of medical services to public and private insurers.
- Internal controlling, auditing, and cost-effective management of treatment.
- Assertion, exercise, or defense of legal claims in connection with treatment.
- Transmission of billing data to private medical clearinghouses (PVS), billing service providers, or factoring service providers that acquire claims against patients or payers and assert them in their own name.

c) Quality assurance and continuing education

- Implementation of quality assurance measures required by law or professional regulations to improve medical care.
- Training and continuing education of medical staff.

d) Compliance with statutory reporting obligations

Processing and transmission of data to fulfill legally mandated reporting obligations, e.g., to public health departments, other competent authorities in accordance with the Infection Protection Act (*IfSG*), or comparable special statutory requirements. Depending on the specific circumstances, the report may be submitted either by us or by the contracted medical laboratory.

e) IT Support and System Administration

- Operation, maintenance, and support of IT systems and specialized medical applications.
- Ensuring the technical availability, functionality, and security of the IT infrastructure (including data backup, access management, and system monitoring).

f) Patient Communication and Practice Management

- Communication with patients, e.g., scheduling appointments, answering questions about treatment, and sharing test results.
- Use of digital or paper-based questionnaires to prepare for and optimize treatment.
- Offering and conducting online video consultations.
- Optimizing and managing internal practice processes and organizational structures.
- Using external communication solutions such as email.

g) Medical documentation

- Documentation of all treatment-related information, such as examination results, diagnoses, treatment courses, and treatment plans.

h) Research and scientific purposes

- Participation in medical studies and scientific research projects.
- Sharing of pseudonymized data with external research institutions or for the publication of scientific findings.

i) Crisis management and emergency care

- Processing of patient data in the context of emergencies, pandemics, or other exceptional crisis situations to protect public health and ensure medical care.

j) Compliance and legal requirements

- Compliance with legal requirements and regulatory obligations (e.g., reporting obligations under the IfSG).
- Conducting internal and external audits to ensure compliance with quality management, data protection, and IT security requirements (e.g., audits).
- Fulfillment of professional obligations in accordance with the professional code of the relevant state medical association (e.g., documentation requirements, retention requirements).
- Implementation of legally required quality management measures.
- Cooperation with regulatory authorities and transmission of data within the framework of legally required audit procedures.
- Verification of and compliance with retention and documentation requirements under applicable laws.
- Processing of data protection requests from data subjects (e.g., requests for information, requests for erasure).

k) Assertion, exercise, and defense of legal claims and demands: The purpose of this processing is to safeguard our legal interests. This includes enforcing our own claims, defending against unjustified claims, and exercising and defending our rights in both extrajudicial and judicial proceedings.

l) Conducting laboratory analyses and medical diagnostics: The purpose of this processing is to ensure comprehensive and high-quality medical diagnostics and care. This includes the analysis of samples in our own laboratory as well as—if necessary—the transfer of samples to specialized external laboratories for additional testing. Such transfers are made exclusively within the scope of the diagnostics required for your treatment.

3. From whom do we receive your data?

We generally collect the data directly from you. In certain cases, we may also receive data from other physicians, medical practices, medical care centers (MVZ), laboratories, clinics, or other medical facilities. Additionally, we may receive your data from third parties, such as government agencies, health insurance companies, or other public health authorities, provided this is legally permissible for the respective purpose.

4. Who has access to your data?

Access to your data is restricted exclusively to those individuals directly involved in your treatment, examination, laboratory analysis, or billing. Processing is carried out only by authorized personnel or under their supervision. This personnel is bound by professional confidentiality and is obligated to maintain confidentiality.

If external medical laboratories are commissioned as part of your diagnostics, they will receive only the information necessary to perform the requested examinations. The specialized staff employed there are also subject to strict data protection regulations and professional confidentiality.

5. What is the legal basis for the processing?

The processing of your data is based on legal requirements to fulfill the treatment contract between you and your physician, as well as the associated obligations. In addition, we rely on further legal grounds that additionally permit us to process your data:

- The processing of **personal master data** (e.g., last name, first name, address, date of birth) is based on Article 6(1)(b) of the GDPR for the purpose of initiating and fulfilling the treatment contract.
- The processing of **all health data in the context of treatment and documentation** is based on Art. 9(2)(h), (3), and (4) of the GDPR in conjunction with § 22(1)(1)(b) 1 No. 1 lit. b) of the Federal Data Protection Act (**BDSG**) and §§ 630a ff. and 630f of the Civil Code (**BGB**). The collection of your data via questionnaires constitutes a pre-contractual measure necessary for the conclusion of the contract with your treating physician.
- The processing for **the administrative handling** of your treatment is based on Art. 6. (1) sentence 1 lit. b) GDPR, Art. 9 (2) sentence 1 lit. h), (3), (4) GDPR in conjunction with § 22 (1) sentence 1 no. 1 lit. b) BDSG in conjunction with § 301 of the Social Code (**SGB**) Book V (**V**) (**SGB V**).
- The **disclosure** of health data to **entities providing joint or follow-up treatment**, such as specialists or laboratories, is carried out for the purpose of medical care on the basis of Art. 9(2)(1)(h), (3), and (4) of the GDPR in conjunction with § 22(1)(1)(b) of the BDSG.
- The processing of data related to **reportable diseases** or laboratory test results in accordance with legal requirements is based on Art. 6. (1) (c) of the GDPR, Art. 9 (2) (h) and (i), (3), and (4) of the GDPR in conjunction with § 22 (1) (1) (b) and (c) of the BDSG.
- Processing for the purposes of **quality assurance in the healthcare sector** is based on Art. 9(2)(1)(i) of the GDPR in conjunction with Sections 299 and 136 of SGB V.
- To the extent that certain data processing operations are based on your explicit **consent**, Art. 6(1)(a) and Art. 9(2)(a) in conjunction with Art. 7 of the GDPR constitute the applicable legal basis. If, in addition, specific statutory requirements apply—such as the German Genetic Diagnosis Act (, **GenDG**) in the case of genetic testing—processing is also carried out on the basis of Section 8 GenDG in conjunction with Article 9(2)(a) and Article 7 of the GDPR. The same applies accordingly to other relevant special laws that contain additional specific requirements for data processing. If we commission a medical laboratory and consent is required for the tests to be performed there, we will also obtain this consent on behalf of the commissioned laboratory. In this case, your consent applies not only to us but also to the commissioned laboratory and, if applicable, to any subcontracted laboratory.
- Processing within the scope of **organizational practice management** (e.g., appointment scheduling, internal processes) is based on Article 6(1)(f) of the GDPR, provided that no overriding legitimate interest to the contrary exists.
- To **fulfill legal obligations**, processing is based on Article 6(1)(c) of the GDPR in conjunction with relevant special statutory provisions.

- In **medical emergencies** where you are unable to give consent (protection of vital interests), processing is carried out in accordance with Article 6(1)(d) and Article 9(2)(c) of the GDPR.
- Processing in the context of **performing public tasks** is based on Article 6(1)(e) and Article 9(2)(g) of the GDPR in conjunction with the Infection Protection Act (*IfSG*), state health laws, or other specific statutory provisions.
- For the processing of data for **scientific research purposes**, we rely on Article 9(2), sentence 1, subparagraphs (h) and (j) of the GDPR and Article 89(1) of the GDPR in conjunction with Sections 27 and 22(1), sentence 1, No. 1, subparagraphs (b) and (c) of the BDSG.
- Processing is carried out in accordance with Article 9(2)(1)(f) of the GDPR if it is necessary for **the establishment, exercise, or defense of legal claims** or if courts are acting within the scope of their judicial activities.
- In the case of **cooperation within the framework of supervisory and control measures**, in particular in connection with financial audits, internal and external audits, proceedings of the Medical Service (MD), data protection audits, or administrative proceedings, the processing is based on Art. 6. (1) sentence 1 lit. c) and f) of the GDPR, Art. 9(2) sentence 1 lit. i) of the GDPR in conjunction with § 22(1) sentence 1 nos. b) and c) of the BDSG.
- For the purposes of **implementing, testing, supporting, and maintaining IT systems and applications**, Article 6(1)(f) of the GDPR, Article 9(2)(i) of the GDPR, in conjunction with Section 22(1)(1)(b) and (c) of the BDSG, apply.

6. Who are the recipients of your data

We transfer your data exclusively within the scope of the purpose for which it is processed and in accordance with applicable data protection regulations.

Recipients of your data may include:

- other treating physicians or clinics (e.g., general practitioner, specialist, consulting physician)
- psychotherapists,
- medical services of health insurance companies;
- associations of panel physicians,
- public or private health insurance companies,
- Accident insurance providers (occupational accident insurance associations),
- private insurance companies (pension, life, and liability insurance, accident insurance
- private medical billing offices or billing centers;
- rehabilitation and therapy facilities;
- Emergency services or ambulance services;
- Public agencies such as public health departments, infection control authorities, and cancer registries;
- Disability assessment offices (e.g., to determine a degree of disability)
- other healthcare or treatment facilities,
- the Medical Service of the Health Insurance Funds,
- medical associations and private medical clearinghouses
- collaborating research institutions,
- Medical laboratories or diagnostic centers;
- Processors (service providers) pursuant to Art. 28 GDPR,
- External quality assurance organizations (data transfer only in pseudonymized form)

- Supervisory or auditing authorities;
- Professionals bound by professional secrecy, such as tax advisors, auditors, and attorneys
- Authorities, such as tax offices or courts
- Payment service providers

In the course of providing our services, we sometimes engage external service providers who act on our behalf. These service providers act as so-called data processors within the meaning of Article 28 of the GDPR. This means that they process data exclusively on our behalf and in accordance with our specific instructions.

All data processors are contractually obligated to comply with data protection regulations, to implement appropriate technical and organizational measures to protect the data, and neither to use the data independently nor to disclose it to third parties. Processing for purposes other than those expressly agreed upon is not permitted.

Processors may include, for example:

- IT service providers (e.g., for maintenance, support, or network security).
- Software providers (e.g., for digital patient forms or online video consultations).
- Hosting or cloud services (e.g., for data storage or server operation).
- Billing or accounting services.

We enter into data protection-compliant agreements with all data processors in accordance with Article 28 of the GDPR, which ensure the lawful processing of data.

In certain cases, your data may be shared within our partner companies. In such cases, we ensure that all participating companies are bound by appropriate data protection agreements (in particular intra-group contracts) to comply with applicable data protection requirements.

7. Is data transferred to third countries?

As a general rule, no data is transferred to entities or individuals outside the European Union (EU) or the European Economic Area (EEA). Should such a transfer nevertheless become necessary, we ensure that the requirements of Articles 44 et seq. of the GDPR are met. This includes, in particular, appropriate safeguards to ensure an adequate level of data protection in the third country.

8. Storage of Your Data

We store your data only for as long as is necessary to carry out the treatment or examination and to fulfill legal or contractual obligations. In addition, different statutory retention periods apply, depending on the type of data and the relevant department. Examples of these include the X-ray Ordinance (RöV) and the Radiation Protection Act (StrlSchG), the Infection Protection Act (IfSG), the Transfusion Act (TFG), the Genetic Diagnostics Act (GenDG), as well as other professional or special legal requirements.

As soon as your data is no longer needed for these purposes and there are no conflicting legal retention obligations, it will be deleted or anonymized in accordance with data protection regulations.

Pursuant to Section 630f(3) of the German Civil Code (BGB) and Section 10(3) of the Model Professional Code for Physicians (MBO-Ä), there is a statutory minimum retention period of 10 years from the conclusion of treatment. Longer retention is permitted if the patient's legitimate interests preclude deletion or if the data is necessary for the assertion, exercise, or defense of legal claims. For civil law reasons—in particular to preserve evidence—retention for up to 30 years may be necessary, as medical liability claims pursuant to Sections 197(1)(1), 199(2), and (3)(2) of the German Civil Code (BGB) become time-barred after 30 years at the latest.

9. How is your data protected?

To protect your data, we implement comprehensive technical and organizational measures that reflect the current state of the art. These include, among other things, data encryption, access control and restriction through role- and permission-based concepts, regular security audits and system checks, as well as data protection and security-related training for our staff. If necessary, your data is further protected by additional

security measures. This may include, for example, the use of special encryption technologies, enhanced access control, or other technical and organizational measures to ensure the highest security standards.

10. What measures are taken when using telemedicine?

When using telemedicine services (video consultations), we implement additional technical and organizational measures to ensure the protection of your data and the confidentiality of medical communications.

We assume your consent to telemedicine services and the associated data processing as soon as you participate in a video consultation. The processing and security of your data always take place in compliance with applicable data protection regulations, IT security requirements, and relevant professional legal regulations.

11. How is the electronic patient record (ePA) handled?

Given the special need for protection of genetic data, genetic findings are not transferred to the electronic patient record.

12. Your rights as a data subject

To the extent that we process data relating to you, you have the following rights under the GDPR to the extent provided by law:

- **access**, in particular to stored data and the purposes of processing (Art. 15 GDPR). This right is limited by the exceptions in Section 34 of the Federal Data Protection Act (BDSG), according to which the right to access information does not apply, in particular, if the data is stored solely on the basis of statutory retention requirements or for data backup and data protection control, if providing the information would require a disproportionate effort, and if misuse of the data processing is prevented by appropriate technical and organizational measures,
- **Rectification** of inaccurate data or completion of incomplete data (Art. 16 GDPR),
- **Erase**, in particular of data that is no longer necessary (Art. 17 GDPR). This right is subject to the restrictions set forth in Section 35 BDSG, according to which the right to erasure may be waived, in particular, if, in the case of non-automated data processing, the erasure would entail a disproportionately high effort and your interest in the erasure is considered to be low,
- **Restriction** of processing (Art. 18 GDPR),
- **Objection** to processing (Art. 21 GDPR),
- **Data portability**, provided that processing is based on consent or is necessary for the performance of a contract or is carried out using automated means (Art. 20 GDPR), as well as
- **Withdrawal** of **consent** you have provided (Art. 7(3)(1) GDPR).
- **Access to your medical records pursuant to Section 630g of the German Civil Code (BGB)**: You have the right to access your complete medical records, provided that no significant therapeutic reasons or the rights of third parties preclude this.

No automated decision-making or profiling within the meaning of Art. 22 GDPR takes place.

Furthermore, you have the option to file complaints

- to our **Data Protection Officer** (by mail to Pfaffplatz 10, 67655 Kaiserslautern, Germany, with the note “Data Protection Officer,” or by email to office@immungenetik-kl.de) or
- to the competent **supervisory authority**

:

The State Commissioner for Data Protection and Freedom of Information, Rhineland-Palatinate

Mailing address:

Visiting address:

P.O. Box 30 40

Hintere Bleiche 34

55020 Mainz

55116 Mainz

Phone: +49 (0) 6131 8920-0

Fax: +49 (0) 6131 8920-299

Email: poststelle@datenschutz.rlp.de

9. Contact Information for the Data Protection Officer

To exercise your legal rights and for questions regarding data processing, you may contact our Data Protection Officer in the manner most convenient for you:

- Email: datenschutz@immungenetik-kl.de
- Mail: Pfaffplatz 10, 67655 Kaiserslautern, with the note “Data Protection Officer”

Your practice team