

Internal Directive of IVF Czech Republic s. r. o. on the Processing and Protection of Personal Data

This Internal Directive on the Processing and Protection of Personal Data addresses the implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as the “GDPR”) within IVF Czech Republic s. r. o. (hereinafter referred to as the “Company”). It therefore sets out the Company's obligations under the GDPR and its activities and responsibilities in its capacity as a personal data controller.

1. PERSONAL DATA CONTROLLER AND PROCESSOR, DATA PROTECTION OFFICER

The controller and processor of personal data is IVF Czech Republic s. r. o., Company ID No. 255 94 575, with its registered office at U Lomu 638, 760 01 Zlín, registered in the Commercial Register maintained by the Regional Court in Brno under File No. C 36412.

The Company determines how personal data will be processed, for what purpose and for how long, unless otherwise stipulated by applicable legislation. The Company is entitled to select additional processors to assist with the processing of personal data.

Data Protection Officer

Questions and comments concerning the processing of personal data, including the withdrawal of explicit written consent, may be sent in writing to Klinika reprodukční medicíny a gynekologie Zlín, U Lomu 638, 760 01 Zlín, or by email to Lenka.Brazdilova@ivfzlin.cz.

The Data Protection Officer has no conflict of interest in connection with the performance of this role.

2. PERSONAL DATA

Personal data means any information relating to an identified or identifiable natural person (i.e. a person who can be identified directly or indirectly on the basis of a set of data).

Personal data may include textual information (e.g. name, personal identification number, telephone number), visual information (e.g. photographs) and online identifiers (e.g. IP addresses, cookies).

Special categories of personal data are also distinguished. These include so-called sensitive data, such as racial origin, religious beliefs, sexual orientation, biometric data, etc.

3. DATA SUBJECT

A data subject is a natural person whose personal data is processed by the Company (job applicants, former employees, patients, suppliers and contractual partners, and visitors to the clinic).

4. PRINCIPLES AND RULES OF PERSONAL DATA PROTECTION

The Company processes all personal data in accordance with the applicable and generally binding legal regulations of the Czech Republic and the GDPR.

All Company employees are familiar with the rules governing data protection, data handling and data security. They are bound by confidentiality obligations and other internal regulations.

The Company regularly conducts internal audits which, among other things, monitor compliance with the rules for handling personal data and the implementation of its personal data protection policy.

All access to personal data is controlled and based on the access rights assigned to individual employees according to their job positions.

Information System (SmartMEDIX® Medical Software)

Each user is assigned a password and specific access rights, which may be granted only by the administrator.

The information system may be used only by employees who have received login credentials authorising them to access the system (physicians, nurses, IVF laboratory staff, coordinators, quality managers and other employees).

Every employee is required to log into the system using their own username and password and to log out after completing their work.

Every entry in medical documentation is uniquely identifiable. The access history makes it possible to identify the user who accessed individual records, the time of access and the workstation from which the data was accessed.

The information system is regularly updated to ensure data integrity. It complies with national data protection requirements (Act No. 264/2025 Coll., on Cybersecurity) and with ČSN EN ISO 15189:2023 (Section 7.6 – Control of Data and Information Management).

All documents and records, including medical documentation maintained in SmartMEDIX and stored on the internal network, are backed up daily on the Company's server and once a week by an external company through remote network administration.

The server is backed up every night to two locations – an external USB drive and a network-attached storage (NAS) device. A backup report is sent to the administrator by email.

A network version of AVG antivirus software is installed on all client workstations. Antivirus protection is configured to operate automatically when receiving emails and opening data files.

5. CATEGORIES OF DATA SUBJECTS

5.1 Job Applicants

5.1.1 Purpose and Legal Basis for Processing Personal Data

The Company processes personal data for recruitment purposes, including offering suitable job positions in the future.

- Personal data necessary for conducting a recruitment process for a specific position – processing is necessary for the performance of a contract pursuant to Article 6(1)(b) of the GDPR.
- Personal data necessary for contacting an applicant – processing is necessary for the purposes of the Company's legitimate interests pursuant to Article 6(1)(f) of the GDPR.
- Protection of persons, health and property (CCTV system) – processing is necessary for the purposes of the Company's legitimate interests pursuant to Article 6(1)(f) of the GDPR.
- No automated decision-making takes place.

5.1.2 Categories of Personal Data

- Identification data used for the accurate, unique and unambiguous identification of the data subject – first name, surname, academic titles, date of birth, permanent residential address, etc.
- Qualification data.
- Contact details – telephone number, mobile telephone number, email address.
- Identification data obtained from the CCTV system.

5.1.3 Categories of Recipients of Personal Data

- The Company.
- Processors operating under a contract, to an appropriate extent.
- Personal data is not transferred to third countries.

5.1.4 Sources of Personal Data

- Personal data obtained directly from job applicants.
- Data obtained from websites and social media.
- CCTV recordings.

5.1.5 Information Provided to Data Subjects

Information is available from the Data Protection Officer and on the website www.ivf-zlin.cz in the document entitled *Processing and Protection of Personal Data*.

Information about the CCTV system is provided through pictograms displayed at the entrances to monitored areas and in a document available from the Data Protection Officer.

5.1.6 Technical and Organisational Measures Adopted

The following measures have been adopted:

- Locked HR office and locked cabinets containing applicants' personal data.
- Qualified employees and appointment of a Data Protection Officer.
- Measures to ensure the ongoing confidentiality, integrity, availability and resilience of systems.
- Data backups and regularly updated antivirus and anti-spam protection.
- Logging of access to the information system.
- Login to the information system using unique usernames and passwords.
- Removal of access rights when an employee is no longer authorised to perform a particular role.
- Logging out of the system after completing work.
- Ability to restore the availability of and access to personal data in the event of a physical or technical incident.
- CCTV system.
- Compliance with the Internal Directive and other regulations governing personal data protection (e.g. the Data Protection and Security Manual).
- Compliance with established work procedures.
- Restriction of access to personal data to authorised persons (HR personnel and Company management).
- Non-disclosure of personal data to third parties, except where required or permitted by law or agreed with the applicant.
- Sending letters containing personal data by registered mail and archiving proof-of-posting receipts.
- Regular security training for employees who have access to applicants' personal data.
- Regular assessments of the effectiveness of the technical and organisational measures implemented.
- Regular audits in accordance with ISO 15189 and ISO 9001.

5.1.7 Planned Periods for Erasure of Personal Data

Immediately after the recruitment process has ended, personal data relating to applicants who have not been employed will be properly destroyed in accordance with the law.

Where an applicant has provided explicit written consent to the retention of their personal data in the personnel database, the personal data may be retained for a period of three years for the purpose of offering suitable employment opportunities.

In justified cases, CVs and related documents may be retained for a maximum period of three years on the grounds of the Company's legitimate interests in the event of legal action brought by an unsuccessful applicant.

Applicants wishing to withdraw their consent to the processing of personal data may do so in writing by email to Ludmila.Presnajderova@ivfzlin.cz or by post to Klinika reprodukční medicíny a gynekologie Zlín, U Lomu 638, 760 01 Zlín.

The CCTV system stores recordings for four to five days, after which they are automatically overwritten.

Live CCTV footage is available to reception staff. Archived recordings may be accessed by the building manager and IT personnel.

5.2 Former Employees

5.2.1 Purpose and Legal Basis for Processing Personal Data

The Company processes personal data for the purpose of maintaining payroll, personnel and related records arising from an employment relationship.

- Personal data necessary for pension and social insurance purposes, etc. – processing is necessary for compliance with a legal obligation pursuant to Article 6(1)(c) of the GDPR.
- Personal data related to the settlement of all obligations towards a former employee (e.g. payment of wages) – processing is necessary for the performance of a contract pursuant to Article 6(1)(b) of the GDPR.
- Personal data necessary for communication with a former employee – processing is necessary for the purposes of the Company's legitimate interests pursuant to Article 6(1)(f) of the GDPR.
- No automated decision-making takes place.

5.2.2 Categories of Personal Data

- Identification data used for accurate, unique and unambiguous identification of the data subject – first name, surname, academic titles, date of birth, permanent residential address, etc.
- Contact details – telephone number, mobile telephone number, email address.
- Payroll data – bank account number.

5.2.3 Categories of Recipients of Personal Data

- The Company.
- Health insurance companies.
- Social security authorities.
- Entities requesting cooperation pursuant to specific legal regulations.
- Legal advisers.
- Processors operating under a contract, to an appropriate extent.
- Personal data is not transferred to third countries.

5.2.4 Sources of Personal Data

- Personal data obtained directly from former employees.
- Personal data obtained in connection with communication with public authorities.

5.2.5 Information Provided to Data Subjects

Information is available from the Data Protection Officer and on the website www.ivf-zlin.cz in the document entitled *Processing and Protection of Personal Data*.

5.2.6 Technical and Organisational Measures Adopted

The following measures have been adopted:

- Locked HR office and locked cabinets containing former employees' personal data.
- Sending letters containing personal data by registered mail and archiving proof-of-posting receipts.
- Qualified employees and appointment of a Data Protection Officer.
- Measures to ensure the ongoing confidentiality, integrity, availability and resilience of systems.
- Data backups and regularly updated antivirus and anti-spam protection.
- Compliance with the Internal Directive and other regulations governing personal data protection (e.g. the Data Protection and Security Manual).
- Compliance with established work procedures.
- Restriction of access to personal data to authorised persons (HR personnel, the finance department and Company management).
- Logging and password protection of access to the information system.
- Prohibition on sharing passwords.
- Removal of access rights when an employee is no longer authorised to perform a particular role.
- Logging out of the information system after completing work.
- Ability to restore the availability of and access to personal data in the event of a physical or technical incident.
- Non-disclosure of personal data to third parties, except where required or permitted by law or agreed with the former employee.
- Regular training for persons who have access to former employees' personal data.
- Regular assessments of the effectiveness of the technical and organisational measures implemented.
- Regular audits in accordance with ISO 15189 and ISO 9001.

5.2.7 Planned Periods for Erasure of Personal Data

Data stored in personnel files is retained for the periods prescribed by applicable legislation.

Documents that are no longer required are destroyed without undue delay.

In justified cases, certain documents are retained for the protection of the employer's rights for the duration of the applicable limitation periods, in view of potential legal proceedings or inspections by administrative authorities.

5.3 Patients

The Company processes the personal data of patients and prospective patients to the extent provided by the data subjects in connection with the provision of healthcare services pursuant to Act No. 372/2011 Coll., on Healthcare Services and the Conditions for Their Provision (Healthcare Services Act), and its implementing regulations; Act No. 373/2011 Coll., on Specific Healthcare Services, as amended; Decree No. 444/2024 Coll., on Medical Documentation; Act No. 296/2008 Coll., on Ensuring the Quality and Safety of Human Tissues and Cells Intended for Human Application and Amending Related Acts (Human Tissues and Cells Act), as amended; and other regulations governing the provision of healthcare services.

In addition, the Company processes personal data obtained in the course of providing healthcare services (e.g. examination results).

5.3.1 Purpose and Legal Basis for Processing Personal Data

- Provision of healthcare services – processing is necessary for compliance with a legal obligation pursuant to Article 6(1)(c) of the GDPR.

- Disclosure of personal data, to the extent strictly necessary, to legal, financial and tax advisers and auditors for the purpose of providing advisory services to the Company – processing is necessary for the purposes of the Company's legitimate interests pursuant to Article 6(1)(f) of the GDPR.
- Protection of patients' lives, health and property and prevention of undesirable acts through CCTV systems – processing is necessary for the purposes of the Company's legitimate interests pursuant to Article 6(1)(f) of the GDPR.
- Protection of life and health through measures adopted in connection with pandemic diseases such as COVID-19 – processing is necessary for the purposes of the Company's legitimate interests pursuant to Article 6(1)(f) of the GDPR.
- No automated decision-making takes place.

5.3.2 Categories of Personal Data

- Identification data used for accurate, unique and unambiguous identification of the data subject (e.g. first name, surname, date of birth, personal identification number, permanent residential address, etc.).
- Contact details (telephone number, mobile telephone number, temporary residential address, email address, etc.).
- Bank account details.
- Data obtained for the purpose of providing healthcare (health-related data).
- Identification data obtained from the CCTV system.
- Patient's body temperature in connection with measures adopted against pandemic diseases such as COVID-19 (as declared by the Chief Public Health Officer of the Czech Republic).

5.3.3 Categories of Recipients of Personal Data

- The Company.
- Health insurance companies.
- Social security authorities (e.g. submission of temporary incapacity-for-work certificates).
- Entities requesting cooperation pursuant to specific legal regulations.
- Legal advisers.
- Healthcare providers involved in additional or follow-up healthcare (e.g. medical laboratories, inpatient facilities).
- Regional Public Health Authority of the Zlín Region in connection with pandemic diseases such as COVID-19 (test results, contact tracing).
- Processors operating under a contract, to an appropriate extent.
- Personal data is not transferred to third countries.

5.3.4 Sources of Personal Data

- Personal data obtained directly from patients.
- Personal data obtained in connection with the provision of healthcare services.
- Personal data obtained in connection with communication with public authorities.
- Data obtained when handling complaints from data subjects.
- CCTV recordings.

5.3.5 Information Provided to Data Subjects

Information is available from the Data Protection Officer and on the website www.ivf-zlin.cz in the document entitled *Processing and Protection of Personal Data*.

Information about the CCTV system is provided through pictograms displayed at the entrances to monitored areas and in a document available from the Data Protection Officer.

5.3.6 Technical and Organisational Measures Adopted

In accordance with the applicable legislation of the Czech Republic, the personal data of patients and prospective patients is processed primarily as part of medical documentation.

Medical documentation is maintained in both paper and electronic form.

Medical records are stored in separate sections of the filing system. Only records for the current year are stored at reception.

Medical records in consulting rooms are kept in opaque folders. During an examination, only the medical record of the patient being examined is placed on the desk.

No medical records are left on the reception counter after working hours. All records are returned to the filing system.

Offices and cabinets containing patients' medical records are kept closed.

Consultations take place in closed rooms, and telephone calls are not answered during consultations.

Examination results are not communicated by telephone.

Letters containing personal data are sent by registered mail, and proof-of-posting receipts are archived.

Access to and exit from the second and third floors are controlled.

Access to the administrative section of the second floor is separated by a door without an external handle.

Visitors may move around the Company's premises only when accompanied by an employee.

A CCTV system is in operation.

Additional measures include:

- Qualified employees and appointment of a Data Protection Officer.
- Measures to ensure the ongoing confidentiality, integrity, availability and resilience of systems.
- Ability to restore the availability of and access to personal data in the event of a physical or technical incident.
- Removal of access rights when an employee is no longer authorised to perform a particular role.
- Data backups and regularly updated antivirus and anti-spam protection.
- Regular updates of the information system.
- Access to medical software only after authentication.
- Access logging and logging out of the information system after completing work.
- Compliance with the Internal Directive and other regulations governing personal data protection (e.g. the Data Protection and Security Manual).
- Compliance with established work procedures.
- Restriction of access to personal data to authorised persons (physicians, nurses, coordinators, other healthcare personnel, the finance department, the healthcare manager and Company management).
- Non-disclosure of personal data to third parties, except where required or permitted by law or agreed with the patient.
- Regular training for relevant employees.
- Regular assessments of the effectiveness of the technical and organisational measures implemented.
- Regular audits in accordance with ISO 15189 and ISO 9001.

The Company also implements current measures adopted in connection with government regulations aimed at combating pandemic diseases such as COVID-19 (body temperature measurement, signing of Declaration Form F 3.32 and Informed Consent Form F 3.33).

5.3.7 Planned Periods for Erasure of Personal Data

The Company processes personal data for as long as necessary to fulfil the relevant purpose and in accordance with the retention and archiving periods prescribed by the applicable legal regulations of the Czech Republic (e.g. Act No. 372/2011 Coll., on Healthcare Services), or for as long as necessary for the establishment, exercise or defence of legal claims.

The CCTV system stores recordings for four to five days, after which they are automatically overwritten.

Live CCTV footage is available to reception staff. Archived recordings may be accessed by the building manager and IT personnel.

5.4 Suppliers and Contractual Partners

The Company processes personal data to the extent provided by data subjects in connection with the conclusion of a contract.

The Company also processes data that is publicly available in public registers.

5.4.1 Purpose and Legal Basis for Processing Personal Data

- Establishment of a contractual relationship – processing is necessary for the performance of a contract pursuant to Article 6(1)(b) of the GDPR.
- Performance of a contract between the Company and a contractual partner (record-keeping, activity monitoring, statistical purposes, etc.) – processing is necessary for the performance of a contract pursuant to Article 6(1)(b) of the GDPR.
- Compliance with statutory obligations under applicable legislation (accounting, advertising regulation, tax obligations, etc.) – processing is necessary for compliance with a legal obligation pursuant to Article 6(1)(c) of the GDPR.
- Sending commercial communications (direct marketing) – processing is necessary for the purposes of the Company's legitimate interests pursuant to Article 6(1)(f) of the GDPR.
- Protection of persons, health and property (CCTV recordings) – processing is necessary for the purposes of the Company's legitimate interests pursuant to Article 6(1)(f) of the GDPR.
- No automated decision-making takes place.

5.4.2 Categories of Personal Data

- Identification data used for accurate, unique and unambiguous identification of data subjects (first name, surname, company name, company identification number, etc.).
- Contact details (telephone number, mobile telephone number, email address, postal address).
- Other data included in contracts, invoices, etc.
- Personal identification number only where required by law.
- Technical data obtained from communication with the data subject (IP address, time of communication).
- Identification data obtained from the CCTV system.

5.4.3 Categories of Recipients of Personal Data

- The Company.
- Entities requesting cooperation pursuant to specific legal regulations.
- Public institutions.
- Legal, financial and tax advisers and auditors for the purpose of providing advisory services.
- Processors operating under a contract, to an appropriate extent.
- Personal data is not transferred to third countries.

5.4.4 Sources of Personal Data

- Data obtained from websites and social media.
- Data obtained during negotiations concerning the conclusion of a contract (including promotional materials and business cards).
- Data obtained during the performance of existing contracts.
- Data obtained when handling complaints from data subjects.
- CCTV recordings.

5.4.5 Information Provided to Data Subjects

Information is available from the Data Protection Officer and on the website www.ivf-zlin.cz in the document entitled *Processing and Protection of Personal Data*.

Information about the CCTV system is provided through pictograms displayed at the entrances to monitored areas and in a document available from the Data Protection Officer.

5.4.6 Technical and Organisational Measures Adopted

The following measures have been adopted:

- Locked offices and locked cabinets containing contracts with suppliers and contractual partners.
- Qualified employees and appointment of a Data Protection Officer.
- Measures to ensure the ongoing confidentiality, integrity, availability and resilience of systems.
- Data backups and regularly updated antivirus and anti-spam protection.
- Login to computers using individual usernames and passwords.
- Removal of access rights when an employee is no longer authorised to perform a particular role.
- Logging out of computers after completing work.
- Ability to restore the availability of and access to personal data in the event of a physical or technical incident.
- Sending letters containing personal data by registered mail and archiving proof-of-posting receipts.
- Controlled access to the second and third floors.
- Separation of the administrative section of the second floor by a door without an external handle.
- Visitors permitted to move around the premises only when accompanied by employees.
- CCTV system.
- Compliance with the Internal Directive and other regulations governing personal data protection (e.g. the Data Protection and Security Manual).
- Compliance with established work procedures.
- Restriction of access to personal data to authorised persons (finance department and Company management).
- Non-disclosure of personal data to third parties, except where required or permitted by law or agreed with the contractual partner.
- Regular training for relevant employees.
- Regular assessments of the effectiveness of the technical and organisational measures implemented.
- Regular audits in accordance with ISO 15189 and ISO 9001.

5.4.7 Planned Periods for Erasure of Personal Data

The Company processes personal data for as long as necessary to fulfil the relevant purpose and in accordance with the periods prescribed by generally binding legal regulations of the Czech Republic, or for as long as necessary for the establishment, exercise or defence of legal claims.

The CCTV system stores recordings for four to five days, after which they are automatically overwritten.

Live CCTV footage is available to reception staff. Archived recordings may be accessed by the building manager and IT personnel.

5.5 Visitors to the Clinic

This category primarily includes visitors attending educational events organised by the Company, prospective patients attending Open Days and visitors to the Company's websites.

5.5.1 Purpose and Legal Basis for Processing Personal Data

- Acquisition of new clients, patients, suppliers, etc. – processing is necessary for the purposes of the Company's legitimate interests pursuant to Article 6(1)(f) of the GDPR.
- Improvement of services for visitors to the websites www.ivf-zlin.cz and www.darovatvajicka.cz and the Company's social media pages – processing is necessary for the purposes of the Company's legitimate interests pursuant to Article 6(1)(f) of the GDPR.
- Protection of persons, health and property (CCTV system) – processing is necessary for the purposes of the Company's legitimate interests pursuant to Article 6(1)(f) of the GDPR.
- No automated decision-making takes place.

5.5.2 Categories of Personal Data

- Identification and contact details obtained during personal meetings – first name, surname, telephone number, mobile telephone number.
- Identification and contact details obtained through completed web forms – first name, surname, email address, telephone/mobile telephone number.
- Cookies – IP address, browser type, selected language, operating system, internet service provider, date and duration of visits to the websites. Cookies used for direct marketing purposes are processed only with the data subject's consent. Websites may also be browsed in a mode that does not allow the collection of personal data.
- Google Analytics services – monitoring the number of visitors and their behaviour on the websites.
- Identification data obtained from the CCTV system.

5.5.3 Categories of Recipients of Personal Data

- The Company.
- Entities requesting cooperation pursuant to specific legal regulations (e.g. the Police of the Czech Republic in cases of suspected administrative or criminal offences).
- Legal advisers.
- Processors operating under a contract, to an appropriate extent.
- Personal data is not transferred to third countries.

5.5.4 Sources of Personal Data

- Personal contact with visitors.
- Data obtained from websites, including contact forms, and from social media.
- CCTV recordings.

Websites

The Company operates the websites www.ivf-zlin.cz, www.darovatvajicka.cz and ivf.travel. It is also active on social media platforms (Facebook, etc.) and processes personal data in the course of its business activities.

Personal data obtained during visits to these websites is processed in accordance with applicable legislation.

To optimise the websites in terms of usability, system performance and the provision of useful information about services, the Company stores and collects information primarily concerning IP addresses, browser types, selected languages, operating systems, internet service providers, and the dates and duration of visits to the websites.

Where the websites contain links to other websites that are not owned or managed by the Company, these rules do not apply to such websites.

The Company may also obtain personal data when visitors complete one of its web forms, including forms relating to:

- Gift vouchers.
- Sperm donation.
- Egg donation.
- Emsella therapy – appointment booking.
- Fotona laser therapy/treatment.
- IVF consultations.
- Infertility treatment.
- Surrogacy.
- Social freezing.
- Male fertility examination packages.

Collectively, these forms collect at least the following personal data: first name, surname, date of birth, age, email address, telephone number and residential address.

In the case of sperm and egg donation, additional information is collected about how the applicant learned about the Company.

In the case of egg donation, information is also collected about whether the applicant has donated eggs before and whether she is currently breastfeeding.

These forms contain various combinations of the personal data listed above.

A completed web form is delivered to the email inbox of a Company employee, who subsequently communicates with the sender.

The applicant's personal data may then be further processed to the extent described above in the Company's electronic database or by a processor with whom the Company has concluded an appropriate contract.

All data is stored digitally for as long as necessary.

Cookies and Their Use

Cookies are generally defined as small data files that are stored in the browser of a device used to access the internet (computer, tablet, smartphone, etc.) when a website is visited, without any active action by the user.

Cookies enable the collection of various types of user data, including information about online behaviour.

Data obtained through cookies is used both to provide internet services and facilitate their further use (e.g. email services, automatic login or pre-filling certain information during online purchases), and to create a form of internet user profile that enables more effective targeting of advertising.

When visitors browse the Company's websites, the Company records their IP address, the duration of the visit and the website from which the visitor arrived.

The Company considers the use of cookies to measure website traffic and customise website display to be within its legitimate interests, as this enables it to provide visitors with better services.

Cookies used for direct marketing purposes are processed only on the basis of the visitor's explicit consent.

Websites may also be browsed in a mode that does not allow the collection of personal data.

The use of cookies may be disabled in the internet browser through the settings provided by the cookie banner informing visitors that the website uses cookies.

The Company also uses Google Analytics to monitor the number of visitors to its websites and their behaviour.

5.5.5 Information Provided to Data Subjects

Information is available from the Data Protection Officer and on the website www.ivf-zlin.cz in the document entitled *Processing and Protection of Personal Data*.

Information about the CCTV system is provided through pictograms displayed at the entrances to monitored areas and in a document available from the Data Protection Officer.

5.5.6 Technical and Organisational Measures Adopted

The following measures have been adopted:

- Locked offices.
- Controlled access to the second and third floors – visitors ring a bell and are admitted by staff.
- Separation of the administrative section of the second floor by a door without an external handle.
- Visitors permitted to move around the Company's premises only when accompanied by employees.
- CCTV system.
- Qualified employees and appointment of a Data Protection Officer.
- Measures to ensure the ongoing confidentiality, integrity, availability and resilience of systems.
- Data backups and regularly updated antivirus and anti-spam protection.
- Regular updates of the information system.
- Login to computers using unique usernames and passwords.
- Removal of access rights when an employee is no longer authorised to perform a particular role.
- Logging out of computers after completing work.
- Ability to restore the availability of and access to personal data in the event of a physical or technical incident.
- Maintenance of access history.
- Sending letters containing personal data by registered mail and archiving proof-of-posting receipts.
- Compliance with the Internal Directive and other regulations governing personal data protection (e.g. the Data Protection and Security Manual).
- Compliance with established work procedures.
- Restriction of access to personal data according to the type of personal data being processed.
- Non-disclosure of personal data to third parties, except where required or permitted by law or agreed with the visitor.
- Regular training for relevant employees.
- Regular assessments of the effectiveness of the technical and organisational measures implemented.
- Regular audits in accordance with ISO 15189 and ISO 9001.

5.5.7 Planned Periods for Erasure of Personal Data

The Company processes personal data for as long as necessary to fulfil the relevant purpose and in accordance with the periods prescribed by generally binding legal regulations of the Czech Republic, or for as long as necessary for the establishment, exercise or defence of legal claims.

The CCTV system stores recordings for four to five days, after which they are automatically overwritten.

Live CCTV footage is available to reception staff. Archived recordings may be accessed by the building manager and IT personnel.

6. INFORMATION ON THE RIGHTS OF DATA SUBJECTS

A data subject has the right to request information from the Company as to whether personal data relating to them is being processed and to obtain access to such personal data.

The data subject also has the right to rectification of their personal data (where personal data is inaccurate or incomplete).

Right to Erasure

The data subject has the right to request the erasure of personal data where one of the following grounds applies:

- The personal data is no longer necessary for the purposes for which it was collected or otherwise processed.
- The data subject withdraws the consent on which the processing is based, and there is no other legal ground for the processing.
- The data subject objects to the processing and there are no overriding legitimate grounds for the processing.
- The personal data has been unlawfully processed.
- The personal data must be erased in order to comply with a legal obligation under European Union or Czech law applicable to the Company.

The processing of personal data in healthcare is generally governed by legal regulations, and this right is therefore limited (e.g. Act No. 372/2011 Coll., on Healthcare Services, and Decree No. 444/2024 Coll., on Medical Documentation).

The right to erasure does not apply in the circumstances described in Article 17(3)(a)–(e) of the GDPR.

Right to Restriction of Processing

The right to restriction of processing may be exercised where:

- The data subject contests the accuracy of the personal data, for a period enabling the Company to verify its accuracy.
- The processing is unlawful, and the data subject requests restriction of the use of the personal data instead of its erasure.
- The Company no longer needs the personal data for the purposes of processing, but the data subject requires it for the establishment, exercise or defence of legal claims.
- The data subject has objected to the processing of personal data. Processing will be restricted until it has been verified whether the Company's legitimate grounds override those of the data subject.

Right to Data Portability

The right to data portability means that the data subject may request to receive or have their personal data transferred where the processing is based on consent (pursuant to Article 6(1)(a) or Article 9(2)(a) of the GDPR) or on a contract pursuant to Article 6(1)(b) of the GDPR, and where the processing is carried out by automated means.

Right to Withdraw Consent

Where personal data is processed on the basis of consent, the data subject has the right to withdraw that consent.

Withdrawal of consent does not affect the lawfulness of processing based on consent given before its withdrawal.

Explicit consent may be withdrawn by sending a request to:

Klinika reprodukční medicíny a gynekologie Zlín
U Lomu 638
760 01 Zlín
Czech Republic

Or by email to the Data Protection Officer: Lenka.Brazdilova@ivfzlin.cz.

Right to Lodge a Complaint

The data subject has the right to lodge a complaint with the supervisory authority, the Czech Office for Personal Data Protection (*Úřad pro ochranu osobních údajů – ÚOOÚ*).

Address: Pplk. Sochora 27, 170 00 Prague 7, Czech Republic

Website: www.uoou.cz

If a personal data breach occurs in connection with the Company's processing activities and results in a high risk to the rights and freedoms of natural persons, the Company will notify the Czech Office for Personal Data Protection without undue delay and publish a notification on its websites.

7. FUNDAMENTAL LEGAL REGULATIONS GOVERNING PERSONAL DATA PROTECTION

- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), effective from 25 May 2018.
- Act No. 110/2019 Coll., on the Processing of Personal Data.
- Act No. 111/2019 Coll., amending certain acts in connection with the adoption of the Personal Data Processing Act.