COOKIES AND PRIVACY POLICY

I. About us

As a responsible organisation that is aware that information has a specific value and is a resource that requires adequate protection, we care to inform data subjects about the processing of personal data properly, especially concerning the provisions on the protection of personal data, including the Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR"). We also make every effort to ensure that patients subject to the requirements set out in the Health Insurance Portability and Accountability Act are provided with health information protection per the HIPAA standards. Therefore, herein we present essential information on the legal basis for the processing of personal data, the methods of their collection and use, as well as the data subjects' rights.

Please be advised that the Controller of your personal data is **DIGITAL PATHOLOGY TEAM WITOLD REZNER spółka komandytowa [limited partnership], offering services under the brand *TwiceView*,** seated in Kielce, registered in the Entrepreneurs' Register of the National Court Registry held by the District Court in Kielce, X Commercial Department, under the number KRS [*National Court Registry no.*] 0000907065, NIP (tax ID): 9592043544, REGON (statistical ID): 389223170. We have appointed a Data Protection Officer, available for you at the following e-mail address: **dataprotection@twiceview.com.**

The personal data are obtained and processed according to the terms and conditions laid down herein.

II. General Provisions

DIGITAL PATHOLOGY TEAM WITOLD REZNER spółka komandytowa is particularly devoted to protecting the privacy of our patients, contractors, partners, subcontractors, providers, employees and associates. Among our priorities, the protection of the rights and freedoms of individuals in connection with processing their personal data occupies a prominent place.

We make sure that the data are processed per the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (hereinafter referred to as "GDPR"), Health Insurance Portability and Accountability Act (HIPAA), the Act of 10 May 2018 on personal data protection, as well as special provisions. These include, among others, the Act of 6 November 2008 on patient rights' Ombudsman, the Act of 28 April 2011 on the health care information system, the Act of 15 April 2011 on health care providers, the Regulation of the Minister of Health of 18 December 2017 on healthcare organisational standards in the field of pathomorphology.

DIGITAL PATHOLOGY TEAM WITOLD REZNER spółka komandytowa is the Controller of personal data within the meaning of GDPR Art. 4 item 7. We also use the services of processing entities, referred to in GDPR Art. 4 item 8, who process personal data on the Controller's behalf (e.g. IT companies, diagnostic software providers, including entities based outside the European Union).

DIGITAL PATHOLOGY TEAM WITOLD REZNER spółka komandytowa implements appropriate technical and organisational measures to ensure a level of security adequate to the possible risk of violating the individual's rights or freedoms of the varying probability of occurrence and the severity of the risk. Our personal data protection activities are based on the adopted policies and procedures and regular training to improve the knowledge and competence of our employees and associates. In addition, HIPAA's Principles of Privacy Practices require us to ensure that all employees, personnel and affiliates, as the case may be, adhere to the privacy protection principles.

III. How do we use your personal data?

If you are our patient, the obligation to deliver personal data results from applicable law and is a prerequisite for providing health services in the field of pathomorphology. That results from GDPR Art. 9 sect. 2 letter h, in connection with applicable law, particularly with the Act of 6 November 2008 on patients' rights and the Patients' Ombudsman, the Act of 28 April 2011 on the health care information system, the Act of 15 April 2011 on medical activity, the Act of 15 April 2011 on health care providers, Regulation of the Minister of Health of 18 December 2017 on healthcare organisational standards in

the field of pathomorphology. We are required to keep medical records, including the identification of our patients using their personal data.

We also process data of persons authorised by the patient to obtain information about their health, namely their name, surname, telephone number, relationship, and address.

As an employer, we process the data of employees and persons who cooperate with us on a basis other than an employment relationship.
Contact details obtained from contractors (e.g. their employees') are used to conclude and efficiently perform contracts.
We use our clients' data to perform the contract and provide our services.
We only share data with third parties upon consent or when we are obliged to do so under the law.

IV. What are our terms and basis for processing your data?

We exercise due diligence to protect the data subjects' interests, and, in particular, we ensure that the data are:

- processed lawfully, fairly and in a manner transparent for the data subject,
- collected for specific, explicit and legitimate purposes and never processed further contrary to these purposes,
- adequate, relevant and limited to what is necessary to achieve the goals for which they are processed,
- correct and updated as necessary. We take measures to ensure that personal data that are incorrect for the purposes of their processing are immediately removed or rectified,
- stored in a form that shall allow identification of individuals they refer to for a period not longer than necessary to achieve the processing objectives;
- processed in a manner ensuring adequate security of the personal data, including protection against unauthorised or unlawful processing and acc
- idental loss or destruction.

V. What are your rights?

We take appropriate measures to provide you with all relevant information in a concise, transparent, understandable and easily accessible form. We communicate with you about the processing of personal data following your right to:

- information provided when obtaining personal data,
- information provided on request - whether the data are processed, and other issues specified in GDPR Art. 15, including the right to a data copy,
- rectification of data,
- being forgotten,
- processing restrictions,
- data transfer,
- objection,
- not to be subject to a decision based solely on automated processing (including profiling),
- information about a data breach.

Also, if your personal data are processed based on your consent, you have the right to withdraw it. The consent may be withdrawn at any time, which shall not affect the legality of the prior processing.

Your data security is our priority. However, if you believe that by processing your personal data, we violate the GDPR provisions, you have the right to lodge a complaint with the President of the Office for Personal Data Protection.

VI. How shall we contact you?

We provide information in writing or otherwise, including, where appropriate, electronically. Upon your request, we can provide information orally, provided that we confirm your identity by other means. If you submit your request electronically, the response will also be provided electronically, where possible, unless you name another preferred form of communication.

VII. When will we fulfil your request?

We try to provide information immediately - as a rule, within one month of receiving the request.
If necessary, this period may be extended by another two months due to the request's complexity. However, in any case, we shall inform you, within one month of receiving your request, of the action taken and (if applicable) an extension of the deadline, stating the reason for such delay.

VIII. Subcontractors/processors

DIGITAL PATHOLOGY TEAM WITOLD REZNER spółka komandytowa may share personal data with entities authorised under the law, encompassing those listed in Art. 26 of the Act of 6 November 2008 on patient rights and Patients' Ombudsman, which include:

1. medical entities providing health services to ensure the continuity of health services;
2. persons being trained for the medical profession to the extent necessary to achieve teaching objectives;
3. universities or research institutes to use for scientific purposes, without disclosing the name and other data enabling the identification of the person to whom the medical records relate;
4. public authorities, including the Patients' Ombudsman, the National Health Fund, associations of medical professions and health care consultants, as well as the Psychiatric Hospital Patients' Ombudsman, to the extent necessary for them to perform their tasks, in particular, supervision and control;
5. Medical Research Agency to the extent specified in the Act of 21 February 2019 on the Medical Research Agency (Journal of Laws, item 447 and of 2020, item 567);
6. the minister in charge of health;
7. courts, including disciplinary courts, prosecutors, medical examiners and professional liability agents in connection with the proceedings; pension authorities and disability assessment teams in connection with their proceedings;
8. entities holding medical services' records, to the extent necessary to keep such records;
9. insurance companies, upon the patient's consent;

10. medical boards subordinate to the minister competent for internal affairs, military medical boards and medical boards of the Internal Security Agency or the Intelligence Agency;
11. medical practitioners, in connection with the procedure for evaluating the health services provider based on the provisions on accreditation in health care or the procedure for obtaining other quality certificates, to the extent necessary to carry them out.

The following persons are authorised to process the data contained in the medical documentation, provide and manage the provision of health services, as well as activities related to the maintenance and security of the ICT system:

1. medical professionals (employed or cooperating with Digital Pathology Team Witold Rezner spółka komandytowa),
2. individuals providing activities auxiliary to health services, as well as activities related to the maintenance and security of the ICT system where medical documentation is processed, based on entrustment contracts under GDPR Art. 28, including companies providing service and support for ICT systems, medical equipment, medical transport, courier and mail services, documentation disposal and other cooperating entities. If we use IT and cloud service providers, we choose those who comply with the Health Insurance Portability and Accountability Act (HIPAA).

We may transfer your personal data to third countries, i.e. countries outside the European Economic Area. However, personal data may only be transferred to third countries or entities for which the European Commission has determined adequate data protection.
The list of countries for which the European Commission issued a decision confirming that the third country provides an adequate level of protection can be found at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#relatedlinks

In the absence of a decision of the European Commission stating the appropriate level of protection specified in GDPR Art. 45 sec. 3, your personal data may be transferred to a third country only on the basis of binding corporate rules, standard data protection clauses adopted by the European Commission, standard data protection clauses adopted by the Polish supervisory authority and approved by the Commission, an approved code of conduct or an approved certification mechanism (GDPR Article 46).

In the absence of a decision from the European Commission stating the appropriate level of protection specified in GDPR Art. 45 sec. 3 or lack of appropriate safeguards specified in GDPR Art. 46, including

binding corporate rules, we will ask you to consent to such transfer to a third country or international organisation, informing you in advance about the risk associated with such transfer pursuant to GDPR Art. 49 sec. 1 letter a.

IX. How we care about the processing of your data

In order to meet legal requirements, we have developed detailed procedures covering such issues as:

- data protection by design and by default,
- data protection impact assessment,
- notification of infringements,
- holding a register of records of processing activities,
- data retention,
- execution of the data subjects' rights.

We regularly check and update our documentation to demonstrate compliance with the legal requirements per the accountability principle laid down in the GDPR. Also, we try to incorporate the best market practices out of concern for the data subjects' interests.

X. Data retention

We return histopathological materials to their donors after the medical service has been performed.

Personal data included in medical documentation is stored in a form that allows identifying individuals they refer to for a period not longer than necessary to achieve the processing objective. After such a period, we shall anonymise (remove any features enabling the identification of a given person) or delete the data. Medical documentation intended for disposal may be issued to the patient or a person authorised by the patient. Within the retention procedure, we limit the period of personal data storage to a strict minimum.

We determine the data processing period primarily based on the law and the Controller's legitimate interest. The retention policy covers data processed in both paper and electronic form.

The period of personal data storage depends primarily on the collection purpose, in accordance with the following criteria:

1. medical documentation shall be stored for 20 years, counting from the end of the calendar year when the last entry was made. In the event of the patient's death as a result of bodily injury or poisoning, the medical records shall be stored for 30 years, counting from the end of the calendar year when the death occurred.
2. the medical documentation with information necessary for monitoring blood and its components handling shall be stored for 30 years, counting from the end of the calendar year when the last entry was made.
3. X-ray images, stored outside the patient's medical records, shall be stored for ten years from the end of the calendar year when the image was taken.
4. medical records for children under two years of age shall be stored for 22 years.

Referrals for examinations or doctor's orders shall be stored for the period of:

1. five years, counting from the end of the calendar year when the health service from the referral or order was provided,
2. two years, counting from the end of the calendar year when the referral was issued - in the event that the health service was not provided due to the patient's failure to arrive at the appointment unless the patient collected the referral.

Data required for accounting and tax settlements will be processed five years from the end of the calendar year when the tax obligation arose.

Your data processed on the basis of consent will be processed until the consent is withdrawn.

XI. Authorisations

We ensure that any person acting under our authorisation and having access to your personal data shall only process it upon our instructions unless other requirements resulting from EU law or the law of a Member State apply.

XII. Decision-making supported by artificial intelligence algorithms, including profiling

Due to the specificity of our business, striving to provide better services, we may use an automated decision-making process regarding the provision of health services in the field of pathomorphology.

1. automated decision-making - this is decision-making regarding a person - based on automated processing (i.e. using software for data analysis, digital image analysis using artificial intelligence algorithms, etc.) without involving people in the decision-making process;
2. profiling - any form of automated processing of personal data, which consists in collecting information about a person (or a group of natural persons and assessing their characteristics or behaviour patterns to qualify them to a specific category or group, in particular, to analyse the disease or health condition).

XIII. Cookies

1. Cookies are IT data, in particular text files, stored in the Website User's end device and intended for using the Website. Cookies usually contain the name of the website they come from, their storage time on the end device and a unique number.
2. Cookies are placed on the Website User's end device by the website owner, who can also access them.
3. The cookie mechanism is not used to obtain any information about website users or track their navigation. Cookies used on the website do not store any personal data or other information collected from users and are used for statistical purposes.
4. The software used for internet browsing (a browser) allows, by default, the use of cookies on the User's device on which it is running. However, in most cases, the software can be configured independently to block any cookies automatically. Cookies settings can be found in the software (web browsers) settings. Please note that setting restrictions on the use of cookies may affect the operation of some website functionalities.
5. Cookies are used to:

- adapt the Website content to the User's preferences and optimise the website use; in particular, these files allow for the recognition of the Website User's device and displaying the website tailored to their individual needs,
- create statistics that help to understand how Website Users use the websites, which helps improve their structure and content,
- maintain the Website User's session (after logging in) by which the User does not have to re-enter the login and password on each page of the Website,

6. The Website uses two basic types of cookies: session cookies and persistent cookies. The session cookies are temporary files stored on the User's end device until logging out, leaving the website or turning the software(web browser) off. The persistent cookies are stored on the User's end device for a specified period determined in the cookies parameters or until deleted by the User.
7. The following types of cookies are used on the Website:
   - "necessary" cookies, enabling the use of the services available on the website, e.g. authentication cookies used for services that require authentication on the website;
   - cookies used to ensure security, e.g. to detect authentication fraud within the Website; "performance" cookies, enabling the collection of information on the website use;
   - "functional" cookies, enabling "remembering" the settings selected by the User and personalisation of the User interface, e.g. in terms of the language or region the User comes from, font size, website look, etc.;
8. The Website owner advises that the website contains links to other websites. In addition, the Website owner recommends reading the privacy policies applicable there, as they are not responsible for them.
9. The website owner's Security Policy (personal data protection) includes a description of technical and organisational security measures. In particular, the following safeguards are applied:
10. Any data collected from users during the registration process are secured with the SSL protocol and through the website access authentication mechanism.