MediCertLab Pleasure of cooperation	Document Code:	MCL_PO_04_02	
	Updated by:	001	2026-05-11
	Reviewed by:	004	2026-05-15
	Approved by:	001	2026-05-18

Privacy Policy

1. Purpose and Scope

This Privacy Policy sets out the rules governing the processing of personal data by MediCertLab Sp. z o.o., hereinafter referred to as “MediCertLab” or the “Controller”.

This Privacy Policy applies to personal data processed in connection with:

- the use of websites operating under the medicertlab.pl and medicertlab.com domains and their subdomains;
- the use of the Online Store, Customer Account, Customer Portal, training and webinar websites, and other systems provided by MediCertLab;
- the submission of orders, enquiries, service requests, applications, complaints and claims;
- the conclusion and performance of contracts and the provision of laboratory testing, design, training, consulting, IT and other services offered by MediCertLab;
- participation in conferences, training courses, workshops, webinars and other events organised or co-organised by MediCertLab;
- the use of contact forms, email, telephone communication, newsletters, satisfaction surveys and other communication channels;
- the use of MediCertLab's social media profiles, external review systems, analytics tools, payment platforms or login features provided by external providers, where such features are available.

This Privacy Policy applies in particular to users of MediCertLab's websites and systems, customers and prospective customers, persons representing customers and suppliers, event participants, recipients of communications, persons submitting enquiries, requests, complaints or claims, and other individuals whose personal data is processed in connection with MediCertLab's activities.

Where personal data is collected directly from the data subject, MediCertLab makes this Privacy Policy or the relevant privacy notice available at the time of collection.

Where personal data has been provided to MediCertLab by a customer, employer, school, university, payer, event partner or another entity, MediCertLab provides the data subject with the required information no later than the first communication with that person or within another period prescribed by law. This obligation does not apply to the extent that the person already possesses the required information or another exemption provided by law applies.

Any entity providing MediCertLab with personal data relating to other individuals should have a lawful basis for doing so and inform those individuals that their data has been shared and that they may consult this Privacy Policy.

For specific forms, services, events or processes, MediCertLab may provide additional or simplified information concerning the relevant purpose of processing. Such information supplements this Privacy Policy and may contain more detailed rules relating to a particular process.

This Privacy Policy does not replace the privacy policies of independent operators of social media services, payment platforms, login systems, webinar platforms or other external services. The processing of personal data by these entities is governed by their own privacy policies.

2. Data Controller and Contact Details

The controller of personal data is MediCertLab Sp. z o.o., with its registered office at 2 Rozwojowa Street, 44-240 Żory, Poland, entered in the Register of Entrepreneurs of the National Court Register under KRS number 0001180362, EU VAT No. PL6511750886 and REGON 542070423, hereinafter referred to as “MediCertLab” or the “Controller”.

For matters concerning the processing of personal data, the rules described in this Privacy Policy and the exercise of data subjects' rights, the Controller may be contacted:

a) by email at: kontakt@medicertlab.pl;

b) by post at the Controller's registered office address specified in paragraph 1.

MediCertLab has not appointed a Data Protection Officer (DPO). Matters concerning personal data protection are handled directly by the Controller using the contact details specified in paragraph 2.

If MediCertLab appoints a Data Protection Officer, the current contact details of the DPO will be made available on the Controller's website, and this Privacy Policy will be updated accordingly.

3. Sources and Categories of Personal Data

MediCertLab may obtain personal data:

- directly from the data subject, in particular through forms, the Online Store, Customer Account, MediCertLab Customer Portal, email, telephone communication, surveys, requests or declarations;
- from a customer, employer, school, university, payer, event partner, co-organiser or another entity registering a participant or providing personal data in connection with the performance of a service;
- from payment service providers, IT system providers, training and webinar platforms, social media services or other external service providers, where the individual uses their features or the transfer of data is necessary for the provision of a service;
- automatically when using MediCertLab's websites and systems, in particular through cookies, technical logs and information relating to devices, browsers and connections.

The scope of personal data processed depends on the nature of the relationship, the service and the purpose of processing. It may include, in particular:

- first name and surname;
- email address, telephone number, postal address and other contact details;
- company or institution name, address, tax identification number (NIP), job title, position or function, and information concerning the represented entity;

- information necessary to create and manage a Customer Account or use the MediCertLab Customer Portal;
- information necessary to conclude and perform a contract, fulfil an order or provide a service;
- payment, settlement and invoice information, as well as information concerning the funding entity, excluding complete payment instrument details processed directly by the payment service provider;
- information contained in service requests, orders, forms, documents provided by the customer and service histories;
- information relating to participation in events, attendance confirmation, issuance of certificates, provision of appropriate organisational arrangements or settlement of funding;
- the content of correspondence, enquiries, requests, complaints, claims, reviews and satisfaction surveys;
- contact details of persons acting on behalf of customers, suppliers, partners or other entities cooperating with MediCertLab;
- technical data, such as IP addresses, online identifiers, browser type, operating system, device information, access times, session information and website activity;
- images, voice recordings or other information recorded during events where the individual may be identified;
- information concerning consent granted or withdrawn, objections raised and communication preferences;
- other data voluntarily provided by an individual or an entity acting on their behalf, where necessary or useful for handling a particular matter.

MediCertLab does not require individuals to provide personal data that is unnecessary for a specific purpose. Persons providing data should limit its scope to information required to fulfil an order, provide a service, organise an event, respond to an enquiry or handle another matter.

As a general rule, MediCertLab does not require the provision of special categories of personal data, such as data concerning health, racial or ethnic origin, religious beliefs, political opinions, trade union membership, genetic data, biometric data used for uniquely identifying a person, or data concerning a person's sex life or sexual orientation.

Where the processing of special categories of personal data becomes necessary for the provision of a specific service, ensuring appropriate conditions for participation in an event or fulfilling a legal obligation, MediCertLab determines the purpose and legal basis of processing, the applicable condition permitting such processing, and provides the individual with the relevant information before collecting the data.

Individuals should not provide MediCertLab with special categories of personal data or data relating to criminal convictions and offences unless such disclosure has been agreed in advance or is necessary for the fulfilment of a specific obligation or the provision of a service.

Where personal data concerning an individual has been provided by a customer, employer, school, university, payer, event partner or another entity, MediCertLab may process, in particular, identification details, contact details, professional information and other data necessary to organise participation, provide a service, maintain communication, process payments or issue a document confirming participation.

4. Purposes and Legal Bases of Processing

MediCertLab processes personal data only to the extent necessary to achieve specific purposes and on an appropriate legal basis.

Personal data may be processed for the following purposes:

Purpose of processing	**Legal basis**
Creating and managing a Customer Account or using the MediCertLab Customer Portal	Article 6(1)(b) GDPR – performance of a contract or taking steps at the request of the data subject prior to entering into a contract
Preparing quotations, accepting and fulfilling orders, providing services or arranging participation in events where the data subject is a party to the contract	Article 6(1)(b) GDPR
Communication and cooperation with employees, representatives, authorised agents and contact persons acting on behalf of customers, suppliers, partners or other organisations	Article 6(1)(f) GDPR – MediCertLab's legitimate interest in establishing and maintaining cooperation, communication and organising the performance of contracts
Handling enquiries and correspondence that do not directly lead to the conclusion of a contract	Article 6(1)(f) GDPR – legitimate interest in maintaining communication and responding to enquiries
Providing laboratory testing, design, training, consulting, IT and other MediCertLab services	Article 6(1)(b) GDPR, where the individual is a party to the contract, or Article 6(1)(f) GDPR, where the individual acts on behalf of or for another entity
Organising events, communicating with participants, confirming attendance, issuing certificates and ensuring appropriate organisational arrangements	Article 6(1)(b) GDPR or Article 6(1)(f) GDPR, depending on the relationship with the participant
Processing payments, issuing and retaining invoices, maintaining accounting and tax records, and fulfilling other legal obligations	Article 6(1)(c) GDPR – compliance with a legal obligation to which MediCertLab is subject
Implementing and settling projects, events or services funded by external entities	Article 6(1)(b), (c) or (f) GDPR, depending on the source of the obligation, funding conditions and relationship with the data subject
Handling requests, complaints and claims	Article 6(1)(b) GDPR, where the matter concerns a contract; Article 6(1)(c) GDPR, where the obligation to handle the matter arises from law; or Article 6(1)(f) GDPR – legitimate interest in protecting MediCertLab's rights and ensuring service quality
Establishing, exercising or defending legal claims and maintaining records that may serve as evidence	Article 6(1)(f) GDPR – legitimate interest in protecting MediCertLab's rights

Ensuring the security of persons, information, IT systems, websites, Customer Accounts and the MediCertLab Customer Portal, preventing misuse and diagnosing technical problems	Article 6(1)(f) GDPR – legitimate interest in ensuring security and business continuity
Conducting satisfaction surveys, assessing service quality, improving event organisation and developing MediCertLab's activities	Article 6(1)(f) GDPR – legitimate interest in evaluating and improving the services provided
Direct marketing of MediCertLab's own products and services	Article 6(1)(f) GDPR – legitimate interest in promoting MediCertLab's activities, subject to the right to object and the requirement to obtain consent for the use of specific communication channels where required by law
Sending newsletters or other marketing communications based on consent	Article 6(1)(a) GDPR and consent required under electronic communications legislation
Using analytics, marketing and social media cookies	Article 6(1)(a) GDPR and the user's consent to storing information on or accessing information from their device
Managing MediCertLab's social media profiles, communicating with users and analysing activity on those platforms	Article 6(1)(f) GDPR – legitimate interest in communication, business promotion and profile management, and Article 6(1)(a) GDPR where consent is required
Recording and publishing identifiable images in documentary, informational or promotional materials	Article 6(1)(a) GDPR and separate consent to the publication of an individual's image, where required
Fulfilling other obligations arising from applicable law or requests from competent authorities	Article 6(1)(c) GDPR

MediCertLab's legitimate interests include, in particular, maintaining ongoing communication, organising cooperation, ensuring the proper provision of services, protecting persons and systems, preventing misuse, assessing service quality, developing business activities, conducting direct marketing of its own products and services, and establishing, exercising or defending legal claims.

Before processing personal data on the basis of legitimate interests, MediCertLab assesses whether those interests are overridden by the interests, rights or freedoms of the data subject.

Providing personal data is voluntary unless its provision is required by law. Certain personal data may be necessary to conclude or perform a contract, create a Customer Account, fulfil an order, issue an accounting document, participate in an event, issue a certificate or respond to an enquiry.

Failure to provide data necessary for a particular purpose may prevent the conclusion or performance of a contract, acceptance of an order, provision of a service, participation in an event, issuance of a document or use of certain website features.

Where processing is based on consent, providing consent is voluntary. Consent may be withdrawn at any time without affecting the lawfulness of processing carried out before its withdrawal.

Email, telephone or other electronic communication methods are used to send marketing communications only after obtaining the consent required by applicable law, regardless of the legal basis for processing personal data under the GDPR.

Individuals may object to the processing of their personal data for direct marketing purposes at any time. Following such an objection, MediCertLab shall cease processing the data for that purpose.

5. Data Recipients and Transfers Outside the EEA

Personal data may be accessed by persons authorised by MediCertLab, exclusively to the extent necessary for the performance of their assigned duties.

Depending on the nature of the relationship, the service provided and the tools used, personal data may be disclosed or entrusted for processing, in particular, to:

- providers of hosting, servers, email services, IT systems, cloud services, the Online Store, Customer Account, MediCertLab Customer Portal, training and webinar systems, and communication tools;
- providers of accounting, legal, payment, banking, insurance, technical, maintenance, marketing, auditing and organisational services;
- carriers, postal operators, delivery service providers and other entities involved in fulfilling orders or providing services;
- testing subcontractors, laboratory service providers, experts, trainers, speakers and other persons or entities involved in providing services;
- partners, event co-organisers, schools, universities, employers, payers and funding institutions, to the extent necessary to organise, conduct or settle an event or project;
- providers of analytics and marketing tools, review systems and social media platform operators, where the relevant feature is used and the required consent has been obtained;
- accreditation, certification, inspection or assessment bodies, auditors and experts involved in assessing MediCertLab's activities, to the extent necessary to conduct the relevant assessment;
- public authorities, courts and other authorised entities, where the obligation or right to disclose data arises from applicable law.

Entities processing personal data on behalf of MediCertLab act under a contract or another appropriate legal instrument and in accordance with MediCertLab's documented instructions.

Certain recipients, particularly payment service providers, banks, carriers, law firms, funding institutions, accreditation bodies and social media platform operators, may process personal data as independent controllers in accordance with applicable law and their own privacy policies.

Personal data may be processed within the European Economic Area (EEA) and, in connection with the use of services provided by certain suppliers, also outside the EEA.

Personal data is transferred to a country outside the EEA or to an international organisation only where permitted under data protection legislation, in particular on the basis of:

- an adequacy decision issued by the European Commission;
- Standard Contractual Clauses approved by the European Commission, together with supplementary safeguards where required;

- Binding Corporate Rules;
- another mechanism provided for under applicable law.

Information concerning data transfers associated with specific analytics, marketing or social media tools may also be made available through the cookie settings panel or the privacy information relating to the relevant tool.

Information about the safeguards applied to transfers of personal data outside the EEA and how to obtain copies of those safeguards may be requested by contacting MediCertLab using the contact details provided in Section 2.

6. Data Retention Periods

MediCertLab retains personal data for as long as necessary to fulfil the purpose for which it was collected and subsequently for the period required by law, MCL's record-keeping requirements or the need to establish, exercise or defend legal claims.

The retention period depends on the nature of the matter and may include, in particular:

- **Customer Account and MediCertLab Customer Portal data** – for the duration of the account's operation and, after its closure, to a limited extent for the period necessary to settle services, fulfil legal obligations and protect against claims;
- **data relating to orders, contracts, service requests or the provision of services** – for the duration of the relevant matter and subsequently for at least 5 years from the end of the year in which the Service was completed, unless a longer period is required by law, contractual terms, laboratory documentation requirements, project or funding conditions, or the applicable limitation period for claims;
- **data forming part of laboratory and technical records, test reports or documentation enabling the course of an order to be reconstructed** – for the retention period applicable to those records, but not less than 5 years, unless a longer period is required by applicable requirements;
- **accounting and tax data, invoices and other settlement documents** – for the period required by law, generally 5 years from the end of the calendar year in which the payment deadline for the relevant tax liability expired, taking into account cases where the limitation period is suspended or interrupted;
- **data contained in enquiries, forms and correspondence that did not result in the conclusion of a contract** – for the duration of the matter and subsequently for no longer than 12 months after the end of communication, unless further retention is justified by the nature of the enquiry, the individual's consent or the need to protect against claims;
- **data relating to complaints, claims, requests or legal disputes** – until the relevant proceedings have been completed and subsequently until the applicable limitation period for claims expires or for the period necessary to demonstrate that the matter was handled correctly;
- **data relating to event participation, attendance lists, issuance of certificates or other confirmations of participation** – for 5 years from the end of the year in which the event took place, unless a longer period is required by funding conditions, a contract or applicable law;
- **data used for project settlement or external funding purposes** – for the duration of the project and its sustainability period, and for the period required for inspections, archiving or settlement as specified by the funding institution or applicable regulations;

- **data from satisfaction surveys and service quality assessments** – for the period necessary to conduct the analysis and implement any resulting measures, generally no longer than 24 months from the date of collection, unless the data is anonymised earlier;
- **data processed for direct marketing purposes** – until an objection is raised, the required consent is withdrawn or the marketing purpose ceases to exist;
- **data concerning consent granted or withdrawn, objections raised and communication preferences** – for the duration of the relevant activity and subsequently for the period necessary to demonstrate MediCertLab's compliance with applicable regulations and protect against claims;
- **identifiable images processed on the basis of consent** – until consent is withdrawn, use of the materials ends or the purpose specified in the image consent declaration ceases to exist, taking into account the rules applicable to materials published before consent was withdrawn;
- **technical logs and system security data** – generally for no longer than 12 months, unless longer retention is necessary to investigate an incident, detect misuse, preserve evidence or protect against claims;
- **data associated with cookies and similar technologies** – for the operational lifetime of the relevant cookie or until consent is withdrawn or the cookie is deleted by the user. The specific retention periods for individual cookies are indicated in the cookie settings panel.

Where the same personal data is processed for several purposes, MediCertLab may retain it until the longest applicable retention period has expired. Once a particular purpose has ended, the data shall no longer be used for that purpose.

Withdrawal of consent, raising an objection, closing a Customer Account or terminating cooperation does not always result in the immediate deletion of all personal data. MediCertLab may continue to retain data where necessary to comply with a legal obligation, document a completed service, settle a contract, demonstrate that consent was granted or withdrawn, or establish, exercise or defend legal claims.

Once the applicable retention period has expired, personal data shall be deleted, anonymised or otherwise processed so that it can no longer be attributed to a specific individual, unless further retention is required or permitted on another legal basis.

Retention periods are reviewed, particularly in the event of changes to applicable law, service delivery methods, systems used or processing purposes.

7. Cookies, Technical Data and Profiling

MediCertLab's websites and systems use cookies and similar technologies that may store information on a user's device or access information already stored on that device.

Depending on their purpose, MediCertLab may use the following categories of cookies:

- **Strictly necessary cookies** – required for the proper and secure operation of the website, session management, login functionality, remembering privacy settings, processing orders or providing features expressly requested by the user;
- **Functional cookies** – enabling selected settings to be remembered and the website's operation to be adapted to user preferences;
- **Analytics cookies** – enabling the compilation of statistics, analysis of website usage, identification of problems and improvement of website performance;

- **Marketing cookies** – used to measure the effectiveness of promotional activities, personalise marketing communications and conduct advertising campaigns;
- **Social media and external content cookies** – enabling the display of content from external services, use of their features or analysis of user activity by their operators.

Strictly necessary cookies may be used without the user's consent where they are required to transmit a communication over a telecommunications network or provide a service expressly requested by the user.

Functional, analytics, marketing, and social media-related cookies are activated only after obtaining the user's consent where such consent is required by law. Until consent has been granted, these technologies remain inactive.

During the first visit to the website, users may use the cookie settings panel to:

- accept all categories of cookies;
- reject cookies other than strictly necessary cookies;
- select individual categories of cookies.

Failure to provide consent or refusal of consent does not restrict access to the website's essential functions. However, it may result in the unavailability of features that rely on technologies requiring consent.

Users may change their settings or withdraw consent at any time through the cookie settings panel available on the website. Withdrawing consent is as easy as giving it and does not affect the lawfulness of processing carried out before its withdrawal.

Users may also manage cookies through their browser settings, including deleting stored cookies, restricting their use or blocking specific technologies. Browser settings do not replace the consent required for non-essential cookies, and changes to these settings may affect the operation of certain website features.

Detailed information about the cookies and similar technologies used, including their names, categories, purposes, providers and operational lifetimes, is available in the cookie settings panel. This list may be updated as the tools used by MediCertLab change.

When using MediCertLab's websites, technical data may be processed automatically, including IP addresses, online identifiers, browser type and version, operating system, device type, language, access time, requested webpage address, referral source, session information and events associated with website usage.

Technical data may be processed to:

- ensure the security of websites, systems and user accounts;
- maintain sessions and ensure the proper operation of available features;
- diagnose errors and technical problems;
- prevent misuse and unauthorised access;
- compile statistics and analyse website usage, after obtaining consent where required;
- conduct and evaluate marketing activities, after obtaining the required consent.

In connection with the use of analytics or marketing cookies, MediCertLab may analyse user activity on the website, including pages visited, actions performed, referral sources and interest in specific content or services.

MediCertLab does not make decisions concerning users based solely on automated processing, including profiling, that would produce legal effects concerning them or similarly significantly affect them.

Where users access content, features or tools provided by external entities, the operators of those services may receive user data and process it in accordance with their own privacy policies. Where a feature requires non-essential cookies, it is activated only after the required consent has been obtained.

MediCertLab's websites may contain links to external websites. Upon accessing an external website, the processing of personal data is governed by the rules established by its operator. MediCertLab is not responsible for the privacy practices of independent operators of such websites.

8. Events, Attendance Lists and Use of Images

MediCertLab may process event participants' personal data for the purposes of organising events, providing organisational communications, confirming participation or attendance, ensuring appropriate participation arrangements, issuing certificates, processing payments or funding, and handling requests, complaints and claims.

Where a participant is registered by an employer, school, university, payer, partner or another entity, MediCertLab may receive identification details, contact information, professional information and other data necessary to organise the participant's attendance. The participant receives information about the processing of personal data in accordance with Section 1 of this Privacy Policy.

MediCertLab may maintain attendance lists or other records confirming participation in an event where necessary for its organisation, issuance of certificates, settlement of funding or demonstration that the service has been provided. The scope of personal data included in such lists is limited to information necessary for the relevant purpose.

Attendance lists are not made available to other participants or published unless this is necessary due to the nature of the event, required by law or funding conditions, or separately agreed with the data subjects concerned.

Where photographs, audio recordings or video recordings are planned during an event, MediCertLab informs participants before the event begins or, at the latest, upon entry to the event venue. Such information may specify, in particular, the purpose of recording, the intended use of the materials and the possibility of objecting to individual photographs or recordings.

Recording the course of an event and retaining documentary materials may be based on MediCertLab's legitimate interests, provided that such processing does not override the rights and freedoms of participants. Public dissemination of an identifiable person's image is additionally subject to the rules arising from legislation protecting image rights.

As a general rule, publishing or otherwise disseminating a photograph or recording in which an identifiable individual is the main subject or is individually featured requires separate, freely given consent. Such consent specifies the purpose, scope, methods and channels of image use and, where necessary, the period for which the image may be used.

Consent to the dissemination of an individual's image is not a condition of participation in an event unless the use of the image is an expressly defined and necessary element of the particular service or event. Refusal to give consent must not result in an unjustified deterioration of participation conditions.

Authorisation to disseminate an individual's image may not be required in cases provided for by law, particularly where the person is merely an incidental element of a larger whole, such as an assembly, public event, landscape or wider view of a location. The applicability of such an exception is assessed on a case-by-case basis, taking into account the nature of the material, its intended use and the rights of individuals visible in the photograph or recording.

This Privacy Policy, acceptance of the Event Terms and Conditions, entry to the event venue or posing for a photograph does not replace separate consent to the dissemination of an individually featured person's image where such consent is required.

Consent to the processing and use of an individual's image may be withdrawn at any time by contacting MediCertLab using the details provided in Section 2. Withdrawal of consent does not affect the lawfulness of activities carried out before its withdrawal.

Following withdrawal of consent, MediCertLab shall cease further use of the individual's image to the extent that consent was the sole legal basis for such use and shall remove the materials from channels under its control where possible and where no other legal basis for continued processing exists. Withdrawal of consent may not make it possible to recall materials previously printed, distributed or saved by independent third parties.

Where the identifiable image of a minor is concerned, the required declarations shall be made by the minor's legal representative. The child's views, welfare and safety shall also be taken into account according to their age and maturity.

Attendance lists, consents and other declarations concerning the use of images may be maintained in paper or electronic form for the period specified in Section 6 and in accordance with MediCertLab's document control procedures.

9. Rights of Data Subjects

Under the conditions and to the extent specified in data protection legislation, data subjects have the following rights:

- **Right of access** – the right to access personal data, obtain information about its processing and receive a copy of the data;
- **Right to rectification** – the right to request correction of inaccurate personal data and completion of incomplete data;
- **Right to erasure** – the right to request deletion of personal data where one of the conditions specified by law applies and there is no legal basis for its continued processing;
- **Right to restriction of processing** – the right to request restriction of the processing of personal data;
- **Right to data portability** – the right to receive and transfer personal data where it is processed by automated means on the basis of consent or a contract;
- **Right to object** – the right to object, on grounds relating to their particular situation, to the processing of personal data based on MediCertLab's legitimate interests;
- **Right to object to direct marketing** – the right to object at any time to the processing of personal data for direct marketing purposes, including related profiling;
- **Right to withdraw consent** – the right to withdraw consent at any time where processing is based on consent, without affecting the lawfulness of processing carried out before its withdrawal;

- **Right not to be subject to automated decision-making** – the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the individual or similarly significantly affects them, subject to exceptions provided for by law;
- **Right to lodge a complaint** – the right to lodge a complaint with the President of the Personal Data Protection Office (Prezes Urzędu Ochrony Danych Osobowych, UODO) where the individual believes that the processing of their personal data infringes data protection legislation.

These rights are not absolute. The ability to exercise them depends, in particular, on the purpose and legal basis of processing, the scope of the request and the legal obligations applicable to MediCertLab.

In particular, the right to erasure may not apply where continued processing of personal data is necessary to:

- comply with a legal obligation;
- establish, exercise or defend legal claims;
- document the performance of a contract, order or service;
- ensure the integrity and retrievability of required laboratory, technical, accounting or other documentation subject to mandatory retention requirements;
- fulfil another purpose permitted by applicable law.

Where an individual objects to processing on grounds relating to their particular situation, MediCertLab shall cease processing personal data on the basis of legitimate interests unless it demonstrates compelling legitimate grounds for processing that override the interests, rights and freedoms of the individual, or grounds for establishing, exercising or defending legal claims.

Where an individual objects to processing for direct marketing purposes, MediCertLab shall cease processing personal data for that purpose.

Requests concerning the exercise of data subject rights may be submitted:

- by email to: kontakt@medicertlab.pl;
- by post to MediCertLab's registered office address specified in Section 2.

The request should contain information sufficient to identify the individual concerned and the right being exercised. Individuals are not required to provide more personal data than necessary to verify their identity and process the request.

Where MediCertLab has reasonable doubts concerning the identity of the person submitting the request, it may request additional information necessary to confirm that person's identity. The scope of information requested shall be limited to what is necessary for this purpose.

MediCertLab shall provide information about the action taken in response to the request without undue delay and, in any event, within one month of receiving it.

Where necessary due to the complexity or number of requests, this period may be extended by a further two months. MediCertLab shall inform the individual of the extension and the reasons for it within one month of receiving the request.

Where MediCertLab does not take action in response to a request, it shall inform the individual of the reasons and of the possibility of lodging a complaint with the President of the Personal Data Protection Office and seeking a judicial remedy.

As a general rule, the exercise of data subject rights is free of charge. Where requests are manifestly unfounded or excessive, particularly because of their repetitive character, MediCertLab may charge a reasonable fee reflecting the administrative costs of handling the request or refuse to act on it, in accordance with applicable law.

A complaint may be lodged with the President of the Personal Data Protection Office without first contacting MediCertLab. However, contacting the Controller beforehand may help resolve the matter more quickly.

10. Data Security

MediCertLab implements appropriate technical and organisational measures to ensure a level of personal data security appropriate to the nature of the processing and the risks involved.

These measures are intended, in particular, to protect personal data against:

- access by unauthorised persons;
- unauthorised or unlawful use, disclosure or alteration;
- accidental loss, destruction or damage;
- loss of availability, integrity or confidentiality;
- other incidents that may adversely affect the rights or freedoms of data subjects.

Depending on the type of system, scope of data and risk assessment, security measures may include, in particular:

- restricting access to personal data according to assigned duties and authorisations;
- using individual authentication credentials and access control mechanisms;
- securing data transmission and connections to systems;
- performing backups and ensuring the ability to restore data and system operations;
- protecting devices, servers, networks, premises and documentation;
- protecting against malware, unauthorised access and other technical threats;
- monitoring system operations and recording security-relevant events;
- granting authorisations, requiring personnel to maintain confidentiality and providing information security training;
- assessing suppliers and concluding appropriate data processing agreements;
- implementing procedures for responding to incidents and personal data breaches;
- periodically reviewing and updating the security measures applied.

Access to personal data is restricted to persons who require it to perform their assigned duties and who have been appropriately authorised or are entitled to access the data under a contract or applicable law.

MediCertLab requires persons with access to personal data to maintain its confidentiality and use it only to the extent and for the purposes related to their assigned tasks.

Where external providers of IT systems, hosting, cloud services or other data processing services are used, MediCertLab selects providers offering appropriate guarantees of data protection and establishes the rules governing processing through a contract or another appropriate legal instrument.

MediCertLab assesses the effectiveness of the security measures applied and, where necessary, adapts them to technological, organisational and legal developments and changes in the level of risk.

MediCertLab maintains procedures for responding to suspected incidents or personal data breaches, including their identification, mitigation, risk assessment, documentation and submission of any required reports or notifications.

Users of the Customer Account or Customer Portal should:

- protect their login credentials against access by third parties;
- not share their passwords with other persons;
- use passwords appropriate to the importance of the account being protected;
- log out after using their account, particularly when using a shared device;
- promptly inform MediCertLab of any suspected unauthorised account access, loss of login credentials or other incident that may affect data security.

For security reasons, MediCertLab does not publicly disclose detailed information concerning system configurations, infrastructure security measures or the protective mechanisms used.

11. Final Provisions

This Privacy Policy constitutes document MCL_PO_04_02 and is published on MediCertLab's websites under the title “Privacy Policy”.

The current version of this Privacy Policy is made available in a manner allowing users to read, save and subsequently reproduce its contents.

The effective date and identification of the current version of this Privacy Policy are specified in the document control information.

This Privacy Policy may be updated, in particular, following changes to:

- the purposes, scope or methods of processing personal data;
- the websites, systems, tools or service providers used;
- the scope of MediCertLab's activities or services;
- applicable laws, guidelines or practices of authorities responsible for data protection;
- the Controller's details or contact methods.

A new version of this Privacy Policy shall take effect on the date specified in its document control information. In the event of significant changes, MediCertLab may communicate them through its website, Customer Account, MediCertLab Customer Portal, email or another appropriate communication channel.

Where MediCertLab intends to process personal data for a new purpose that is incompatible with the purpose for which it was originally collected, it shall provide the data subject with the information required by law and ensure an appropriate legal basis before commencing such processing.

Previous versions of this Privacy Policy may be retained by MediCertLab to demonstrate the content of the information applicable during a particular period and compliance of data processing with applicable requirements.

Matters not regulated by this Privacy Policy shall be governed by the relevant provisions of data protection legislation.