

ZM CRO GROUP® POLICY (ПОЛИТИКА)

TITLE:	Confidentiality Policy Политика Конфиденциальности
INDEX CODE:	BP06-POL-19
VERSION NUMBER:	1.0
EFFECTIVE DATE:	01-Mar-2024* *05-Фев-2026 выполнен перевод Политики на русский язык для веб-сайта www.zmcro.com.
DUE DATE FOR SCHEDULED REVISION:	01-Mar-2026

SIGNATORIES / ПОДПИСИ

ROLE / РОЛЬ	NAME, TITLE /ФИО, ДОЛЖНОСТЬ	SIGNATURE / ПОДПИСЬ	DATE / ДАТА
AUTHOR / РАЗРАБОТАЛ	Elena Gurova, Development Director, Quality Assurance Manager of ZM CRO GROUP® Елена Гурова, Директор по развитию, Менеджер по обеспечению качества		06-Feb-2026 06-Фев-2026
REVIEWER / ПРОСМОТРЕЛ	Yuri Zaretsky, CEO of ZM CRO GROUP® Юрий Зарецкий, учредитель		06-Feb-2026 06-Фев-2026
APPROVER / УТВЕРДИЛ	Yuri Zaretsky, CEO of ZM CRO GROUP® Юрий Зарецкий, учредитель		06-Feb-2026 06-Фев-2026

I. PURPOSE / ЦЕЛЬ

This Confidentiality Policy (hereinafter, the “Policy”) provides guidelines for employees, contractors, and third parties handling confidential information towards pharmacovigilance services in clinical trials and post-marketing surveillance. The Policy protects sensitive information of the ZM CRO GROUP®, clients, and employees by limiting access, use, and disclosure to authorized individuals only.

Данная Политика конфиденциальности (далее по тексту – «Политика») является руководством для сотрудников, подрядчиков и третьих лиц, которые вовлечены в обработку конфиденциальной информации в рамках услуг по фармаконадзору в клинических исследованиях и пост-маркетинговом надзоре. Данная Политика направлена на защиту информации для служебного пользования ZM CRO GROUP®, ее клиентов и сотрудников посредством ограничения доступа, использования и раскрытия информации уполномоченным лицам.

II. SPHERE OF APPLICATION / ОБЛАСТЬ ПРИМЕНЕНИЯ

This Policy applies to all operations performed by the Data Processor/Operator with Personal Data on behalf of Data Controller (e.g. MAH, Sponsor, CRO, etc.), if and where applicable, and to all employees, contractors, and third parties of ZM CRO GROUP® who have access to Personal Data in any form, including electronic, written, verbal, or visual information. It is applicable to all departments and levels within the ZM CRO GROUP® and must be adhered to at all times.

Данная Политика применима ко всем действиям с персональными данными, которые совершает Оператор или лицо, выполняющее обработку персональных данных от имени и по поручению Контролера (Оператора - для РФ)¹ (например, от лица ДРУ, Спонсора, КИО, другое), если это применимо, а также ко всем сотрудникам, подрядчикам и третьим лицам ZM CRO GROUP®, которые имеют доступ к персональным данным в любой форме, включая электронную, письменную, устную, или информацию в виде изображений (визуальную). Данная Политика применима ко всем департаментам и на всех уровнях ZM CRO GROUP® и должна соблюдаться на любом этапе работы с информацией (дынными).

III. DEFINITIONS / ОПРЕДЕЛЕНИЯ

Anonymized data – data rendered anonymous in such a way that the data subject is not or no longer identifiable.

Обезличенные (анонимизированные данные) – данные, которые были обработаны таким образом, что субъект персональных данных не может быть идентифицирован.

¹ В рамках Российского законодательства термин «Контролер» следует трактовать как «Оператор».

Anonymization of personal data – actions performed on personal data that do not permit the identity of the individual concerned to be verified solely from such anonymized data.

Обезличивание (анонимизация) персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

Consent of the data subject – any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Согласие субъекта персональных данных – любое свободно данное, конкретное, информированное и недвусмысленное указание на желание субъекта данных, посредством которого он или она выразил(а) согласие на обработку относящихся к нему/к ней персональных данных. (Примечание: более детальное определение «согласия» регламентировано ст.9 Федерального закона от 27.07.2006 №152-ФЗ (в действующей редакции) «О персональных данных».

Contingent worker – person who is contacted for contingent work, paid according to hours worked or fixed salary, and draws no benefits that are commonly available to the regular employees. contingent worker can be an individual/freelancer or freelancer with a company for a taxation purpose working on behalf of ZM CRO GROUP® on the base of contractual agreement. synonymous with independent contractor.

Временный работник – лицо, с которым заключен договор на временную работу, оплачиваемую в соответствии с отработанными часами или фиксированной заработной платой, и не получает никаких льгот, которые как правило предоставляются обычным сотрудникам. Временный работник может быть физическим лицом/фрилансером или внештатным сотрудником компании, работающим от имени ZM CRO GROUP® на основе договора. это синоним «независимого подрядчика».

Data operator / processor² – state agency, municipal authority, legal entity or individual who independently or in cooperation with other entities organizes and/or processes personal data as well as determines the purposes and scope of personal data processing. This definition refers, depending on the context, to any single company of ZM CRO GROUP® or to all ZM CRO GROUP® Companies.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными Данное определение относится, в зависимости от контекста, к какой-либо отдельной организации, входящей в состав ZM CRO GROUP®, или к ZM CRO GROUP® в целом.

Data subject – any natural person, whose personal data is being processed, e.g. employee, clinical trial participants/subjects, investigator, representative of the Sponsor or any other natural person.

Субъект персональных данных – это любое физическое лицо, чьи персональные данные обрабатываются, например, сотрудник, субъект клинического исследования, исследователь, представитель Спонсора или любое другое физическое лицо.

Employee – a person who has been hired for a position or a specific job or project (contract employee).

Сотрудник – лицо, с которым заключен трудовой договор на определенную должность или для выполнения конкретной работы или проекта (сотрудник по контракту).

Health data – personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Медицинские данные – персональные данные, относящиеся к физическому или психическому здоровью физического лица, включая предоставление медицинских услуг, которые раскрывают информацию о состоянии его здоровья.

Pseudonymization (coded data) – the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.

Псевдонимизация (закодированные данные) — это метод защиты персональных данных, при котором персональные данные (например, имя, фамилия, адрес) заменяют на псевдоидентификаторы (например, номер или код) таким образом, чтобы персональные данные субъекта не позволяли отнести данные к конкретному субъекту без использования дополнительной информации.

Personal data – any information about a natural person who is identified or whose identity is directly or indirectly identifiable (hereinafter referred to as "personal data subject"), e. g. by name and surname, a personal identification number, location data and an online identifier or by physical, physiological, genetic, mental and other features.

² Under GDPR, a Data Controller is an organization or individual that decides how and why personal data will be processed. A Data Processor is any third party that processes Personal Data on behalf of a Data Controller. A data processor must only process personal data as instructed by the data controller, unless required to do so by law.

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных), например, имя, фамилия, ИНН, данные о местонахождении, онлайн-идентификаторы или по физическим, физиологическим, генетическим, психическим и другим особенностям.

Personal data processing – any action (operation) or a combination of actions (operations) performed both automatically and manually with personal data, including collection, recording, arrangement, accumulation, storage, specification (updating, changing), extraction, use, distribution (including transfer), anonymizing, blocking and destruction of personal data.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Responsible person – a person responsible for the protection of personal data and appointed by the controller, including a DPO. E-mail of the DPO appointed by the controller: data.protection@zmcro.com.

Ответственное лицо – лицо, ответственное за защиту персональных данных и назначенное оператором, включая должностное лицо по защите данных. Адрес электронной почты должностного лица по защите персональных данных: data.protection@zmcro.com.

Special categories of personal data – data related to racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, etc.

Специальные категории персональных данных – сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, другое.

Vendor – person or company contracted by ZM CRO GROUP® to provide services or assure the functions related to ZM CRO GROUP® or specific project's activities.

Поставщик услуг – лицо или организация, которая в рамках договоров с ZM CRO GROUP® предоставляет услуги или выполняет функции или активности в проектах ZM CRO GROUP®.

Distribution of personal data – actions related to making the data available to indefinite range of persons.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Provision of personal data – actions related to making the data available to a definite person or a definite range of persons.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Blocking of personal data – the temporary cessation of personal data processing (except for the cases when the processing is needed for personal data specification).

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Destruction of personal data – actions performed on personal data contained in the respective database that prevent such data from being restored and (or) actions aimed at the physical destruction of the tangible medium of personal data.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в системе и (или) в результате которых уничтожаются материальные носители, содержащие персональные данные.

Cross-border transfer of personal data – cross-border transfer of personal data to a foreign state agency, foreign legal entity or individual located in a foreign state.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

CRO – Contract Research Organization / КИО – Контрактно-исследовательская организация.

CDA – Confidentiality and Disclosure Agreement / СОК – Соглашение о конфиденциальности.

DPA – Data Processing Agreement / СОД – Соглашение об обработке данных.

MAH – Marketing Authorization Holder / ДРУ – Держатель регистрационного удостоверения.

NCA – National Regulatory Authorities / НРО – Национальный (локальный) уполномоченный регуляторный орган.

IV. POLICY / ПОЛИТИКА

A. Rights and obligation of Data Controller / Права и обязанности Контролера

Data Controller has a right to / Контролер данных имеет право:

- determinate the purposes and means of processing Personal Data.
Установить цели и методы обработки персональных данных.

Data Controller is obliged to / Контролер данных обязан:

- take into account the purpose, nature, context, and scope of any data processing activities.
учитывать цели, характер, контекст и объем при обработке персональных данных.
- consider the likelihood of any severe risk to the freedoms and rights of any natural persons.
учитывать любую вероятность риска нарушения прав и свобод любого физического лица.
- implement appropriate organizational and technical measures and security measures that demonstrate that the data processing activities have been performed in accordance with local regulations.
внедрять надлежащие организационные и технические меры и меры обеспечения безопасности, гарантирующие, что обработка персональных данных выполняется в соответствии с локальными нормативно-правовыми актами.
- review and update these measures where necessary.
пересматривать и обновлять указанные выше меры, при необходимости.
- notify the competent supervisory authority of any breach likely to endanger individuals' rights and freedoms without undue delay.
уведомлять компетентные надзорные органы о любых нарушениях, которые могут поставить под угрозу права и свободы физических лиц.
- appoint a Data Protection Officer, when necessary.
назначить должностное лицо по защите персональных данных.
- perform data protection impact assessment.
проводить оценку воздействия на систему защиты персональных данных.

B. Rights and obligation of Data Operator / Processor / Права и обязанности Оператора / или лица, осуществляющего обработку персональных данных от имени и по поручению Оператора

The Operator/Processor has the right to / имеет право:

- receive reliable information and/or documents containing Personal Data from the Data Subject.
получать от Субъекта достоверную информацию и/или документы, содержащие персональные данные.
- require the Data Subject to clarify the provided personal data in a timely manner.
требовать от Субъекта своевременного уточнения предоставленных персональных данных.
- engage Sub-Processors to carry out specific tasks, in this case Operator/Processor must have a written agreement with the Sub-Processor that imposes the same data protection obligations as stated in the DPA between the Data Controller and the Data Operator / Processor.
привлекать суб-операторов для выполнения конкретных задач. В этом случае Оператор/Обработчик данных должен иметь письменное соглашение с суб-оператором, которое устанавливает те же обязательства по защите данных, которые указаны в Соглашении о защите персональных данных между Контролером и Оператором / лицом, осуществляющим обработку персональных данных от имени и по поручению Оператора.

The Operator/Processor is obliged to / обязан:

- process Personal Data in accordance with the procedures established by the current legislation (global and/or local).
обработать персональные данные в соответствии с процедурами, установленными действующим законодательством (глобальным и/или локальным).
- consider the requests of the Data Subject regarding the processing of Personal Data and provide motivated answers.
рассматривать запросы Субъекта, касающиеся обработки его персональных данных, и предоставлять мотивированные ответы.
- provide the Data Subject with the possibility of free access to his/her Personal Data.
предоставлять Субъекту возможность свободного доступа к его персональным данным.
- take measures to clarify and destroy the Personal Data of the Data Subject in connection with his/her (his/her legal representative's) treatment of legitimate and reasonable demands.
принять меры по уточнению или уничтожению персональных данных Субъекта в связи с выполнением им (его законным представителем) законных и обоснованных требований.
- organize the protection of Personal Data in accordance with the requirements of the current legislation (global and/or local).
организовать защиту персональных данных в соответствии с требованиями действующего законодательства (глобального и/или локального).
- assist the Data Controller in fulfilling their obligations under the law.
оказывать содействие Контролёру данных в выполнении им своих обязательств в соответствии с законом.
- appoint a Data Protection Officer, when necessary.
назначить должностное лицо по защите персональных данных.
- notify the Data Controller of any breach likely to endanger individuals' rights and freedoms without undue delay.
немедленно уведомлять Контролёра о любом нарушении, которое может поставить под угрозу права и свободы физических лиц.
- ensure that international transfers of Personal Data are comply with the local law.
обеспечивать выполнение требований локальных нормативно-правовых актов в случае трансграничной передачи персональных данных.
- publish or provide otherwise unrestricted access to this Policy.

публиковать или иным образом предоставлять неограниченный доступ к настоящей Политике.

C. Rights and obligation of Data Subjects / Права и обязанности Субъектов персональных данных

Data Subjects have the right to / Субъект персональных данных имеет право:

- obtain a full information about their Personal Data processed by the Operator/Controller.
получать полную информацию о своих персональных данных, обрабатываемых Оператором/Контролером.
- access their Personal Data, including the right to receive a copy of any record containing their Personal Data, except in cases provided for by the law.
получать доступ к своим персональным данным, включая право на получение копии любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законом.
- clarify, send the request to block or destroy their Personal Data in cases where the personal data is incomplete, outdated, inaccurate, illegally obtained or is not necessary for the stated purpose of processing.
уточнять, направлять запросы на блокирование или уничтожение своих персональных данных в случаях, когда персональные данные являются неполными, устаревшими, неточными, получены незаконным путем или не являются необходимыми для заявленной цели обработки.
- withdraw consent to the processing of Personal Data.
отозвать согласие на обработку персональных данных.
- take legal measures to protect their rights.
принять законные меры для защиты своих прав.
- exercise other rights in accordance with local laws.
осуществлять другие права в соответствии с локальным законодательством.

Data Subjects are obliged to / Субъект персональных данных обязан:

- provide the Operator/Controller with only reliable information about yourself.
предоставлять Оператору/Контролеру только достоверную информацию о себе.
- provide documents containing Personal Data to the extent necessary for the purpose of processing.
предоставлять документы, содержащие персональные данные, в объеме, необходимом для установленных целей обработки.
- inform the Operator/Controller about the clarification (updating, modification, etc.) of their Personal Data.
информировать Оператора/Контролера об уточнении (обновлении, модификации и т.д.) своих персональных данных.

V. GUIDELINES and PROCEDURES / РУКОВОДЯЩИЕ ПРИНЦИПЫ И ПРОЦЕДУРЫ

5.1 Scope and categories of Personal Data processed, categories of Data Subjects / Состав (объем) и категории обрабатываемых персональных данных, категории Субъектов:

5.1.1 Scope of Personal Data processed / Состав (объем) обрабатываемых персональных данных:

- **Employees' Personal Data** for internal administration and service provision (Name, Last name; Personal Code/National Identification Number; Social Security Number; Number, Date of Expiry and Authority of ID/Passport (copy/photocopy of ID/Passport); Residence address; Personal phone number; Bank account number; Salary; Health data (a medical certificate, e.g. 086-u form, if applicable); Another information that must be processed in the labor relations related context (e.g. copies of certificates).
Персональные данные сотрудников, обрабатываемые для внутренних административных целей и оказания услуг (ФИО, ИНН, СНИЛС, паспортные данные, адрес, номер телефона, банковские реквизиты, данные о размере оплаты труда, данные о здоровье (медицинские сертификаты, например, справки по форме 086-у, если применимо), другая информация, которая должна быть обработана в контексте трудовых отношений.
- **Personal Data from Clinical trial**³ (Investigators' Personal Data (such as name, last name, contact details, place of employment, specialty, professional qualifications and experience in clinical trials, and comments on clinical trial activity).
Персональные данные из клинических исследований (персональные данные исследователей (такие как ФИО, контактные данные, место работы, специальность, квалификация и опыт работы в клинических исследованиях, и другая информация в рамках деятельности по клиническим исследованиям).
- **Personal Data in Pharmacovigilance** received directly from patients or from other sources (medical representatives, health care professionals, literature, social networks and etc. (e.g. patient ID number/initials, date of birth/age, gender, ethnic origin, information about adverse event / reaction (e.g. symptoms, duration, outcome, suspected drug/device, concomitant medication, medical history), contact details of patient or reporter for follow-up if agreed with MAH (refer to GVP Module VI)).
- **Персональные данные в рамках деятельности по фармаконадзору**, полученные напрямую от пациентов и из других источников (медицинских представителей, врачей, литературы, социальных сетей, и т.д. (например,

³ ZM CRO GROUP® does not obtain and process the Personal Data of Trial Subjects in Clinical trials. ZM CRO GROUP® team should ensure that Investigators are aware that only anonymized (pseudonymized (coded)) trial Subject Personal Data can be provided to ZM CRO GROUP®.

Команда ZM CRO GROUP® не получает и не обрабатывает персональные данные субъектов клинических исследований. Команда ZM CRO GROUP® должна уведомить исследователей о том, что ZM CRO GROUP® могут быть предоставлены только анонимизированные (псевдонимизированные (закодированные)) персональные данные субъектов исследования.

идентификационный код пациента / инициалы, дата рождения / возраст, пол, этническая принадлежность, информация о нежелательном явлении / реакции (в том числе симптомах, продолжительности, исходе, подозреваемых лекарственных препаратах/медизделиях, сопутствующей терапии, медицинском анамнезе), контактные данные пациента или репортера для сбора дополнительной информации, если согласовано с ДРУ (в соответствии с Надлежащей практикой фармаконадзора)).

5.1.2 Categories of Data Subjects / Категории Субъектов:

- Staff (e.g. employees, consultants, temporary workers, etc.).
Персонал (например, сотрудники, консультанты, временные работники, другое).
- Business partners (e.g., manufacturers, distributors, medical representative, etc.), clients and vendors.
Бизнес-партнеры (например, производители, дистрибьюторы, медицинские представители, другое), клиенты и поставщики услуг.
- Consumers (e.g. patients, healthcare professionals, etc.).
Потребители (например, пациенты, врачи, другое).
- Regulatory Authorities.
Регуляторные органы.

5.2 Purposes of Personal Data collection / Цели сбора персональных данных:

- maintaining personnel and accounting records, registration of labor and civil relations.
ведение кадрового и бухгалтерского учета, оформление трудовых и гражданско-правовых отношений.
- provision of pharmacovigilance and safety management services, including communications, performance or supervision of the collection and processing of adverse events/adverse drug reactions/special situation reports, follow-up information from various sources (literature and Internet, healthcare professionals, consumers, medical and/or pharmaceutical representatives, etc.), expedited and periodic reporting to NCA, hosting and maintenance of automated certified safety database, safety trends and signal detection, monitoring and management, etc.
предоставление услуг по фармаконадзору и управлению безопасностью, включая коммуникацию, выполнение или надзор за сбором и обработкой сообщений о нежелательных явлениях / реакциях на лекарственные препараты / особых ситуациях, сбора последующей информации о случае из различных источников (литература и Интернет-ресурсы, врачи, потребители, медицинские и/или фармацевтические представители и т.д.), экспресс-отчетность и периодическую отчетность в НРО, хостинг и поддержание автоматизированной сертифицированной базы данных по безопасности, трендов по безопасности и обнаружение, мониторинг и управление сигналами, и т.д.
- implementation of other functions, powers and obligations assigned to the Operator/Processor.
выполнение других задач, полномочий и обязанностей, возложенных на Оператора/лицо, осуществляющее обработку персональных данных от имени и по поручению Оператора.

5.3 Legal basis for the processing of Personal Data / Правовые основания для обработки персональных данных:

- Good pharmacovigilance practice.
Надлежащая практика фармаконадзора.
- Good clinical practice.
Надлежащая клиническая практика.
- GDPR / Общий регламент по защите данных ЕС – не применимо для РФ.
- GCDMP.
Надлежащая практика управления клиническими данными
- Labore code.
Трудовой кодекс.
- Local data protection regulatory requirements and guidelines.
Локальные нормативно-правовые требования и рекомендации в отношении защиты персональных данных.
- Agreements concluded between the Operator and Data Subject (if applicable).
Соглашения, заключенные между Оператором и Субъектом персональных данных (если применимо).
- Consent of personal data subjects to the processing of Personal Data.
Согласие субъектов на обработку персональных данных.
- Other grounds when consent to the processing of Personal Data is not required by law.
Другие основания, когда согласие на обработку персональных данных не требуется по закону.

5.4 Procedures and conditions of Personal Data processing / Порядок и условия обработки персональных данных:

5.4.1 The processing of Personal Data by the Operator is carried out in the following ways / Обработка персональных данных может осуществляться следующими способами:

- without using automation tools / без использования средств автоматизации;
- in information systems with or without transmission of the received information via information and telecommunication networks / в информационных системах с передачей полученной информации по информационно-телекоммуникационным сетям или без нее;
- mixed processing of Personal Data / смешанная обработка персональных данных.

5.4.2 List of actions performed by the Operator with Personal Data includes: collection, systematization, accumulation, storage, clarification (updating, changing), use, distribution (including transfer), pseudonymization, blocking, destruction, as well as carrying out any other actions in accordance with the global and local legislation.

Перечень действий, выполняемых Оператором с персональными данными, включает: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (включая передачу), псевдонимизацию, блокирование, уничтожение, а также осуществление любых других действий в соответствии с международным и локальным законодательством.

5.4.3 The processing of Personal Data is carried out by the Operator subject to obtaining the **Consent of the Data Subject** (hereinafter referred to as "Consent"), with the exception of cases established by the local legislation when the processing of Personal Data can be carried out without such Consent.

Обработка Персональных данных осуществляется Оператором при условии получения Согласия Субъекта данных (далее – «Согласие»), за исключением случаев, установленных локальными нормативно-правовыми актами, когда обработка персональных данных может осуществляться без такого согласия.

5.4.4 The Data Subject decides to provide his/her Personal Data and gives his/her Consent freely, of his/her own free will and in his/her own interest. Consent to the processing of Personal Data may be given by the Data Subject or their representative in any form that provides evidence of its receipt, unless otherwise stipulated by local law.

Субъект принимает решение о предоставлении своих персональных данных и дает свое согласие свободно, по собственной воле и в своих собственных интересах. Согласие на обработку персональных данных может быть дано Субъектом или его представителем в любой форме, подтверждающей его получение, если иное не предусмотрено локальными нормативно-правовыми актами.

5.4.5 When processing Personal Data, the Operator takes or ensures that the necessary **legal, organizational and technical measures** are taken to protect Personal Data from unlawful or accidental access, destruction, alteration, blocking, copying, provision, dissemination of personal data, as well as from other unlawful actions in relation to Personal Data.

При обработке персональных данных Оператор принимает или обеспечивает принятие необходимых правовых, организационных и технических мер для защиты персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных.

5.4.5.1 These measures shall include as appropriate (without limitations) / Меры могут включать (без ограничений):

- the pseudonymization and encryption of Personal Data.
псевдонимизация и шифрование персональных данных.
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
возможность непрерывного обеспечения конфиденциальности, целостности, доступности и отказоустойчивости систем и сервисов обработки.
- the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident.
возможность своевременного восстановления доступности и доступа к персональным данным в случае инцидента.
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
внедрение процесса регулярного тестирования, оценки результативности технических и организационных мер по обеспечению безопасности данных.

5.4.6 The condition for terminating the processing of Personal Data may be the achievement of the purposes of processing Personal Data, expiration of the Consent or withdrawal of Consent by the subject of Personal Data, as well as identification of unlawful processing of Personal Data.

Условием прекращения обработки персональных данных может быть достижение цели их обработки, истечение срока действия Согласия или отзыв Согласия Субъектом персональных данных, а также выявление фактов незаконной обработки персональных данных.

5.4.7 Consent may be revoked by written notice sent to the ZM CRO GROUP® via corporate email info@zmcro.com.

Согласие может быть отозвано путем направления письменного уведомления в ZM CRO GROUP® по корпоративной электронной почте info@zmcro.com.

5.5 Updating, correction, removal and destruction of Personal Data, responding to requests for access to Personal Data by Data Subjects / Обновление, исправление, удаление и уничтожение персональных данных, ответы на запросы Субъектов о предоставлении доступа к персональным данным:

5.5.1. If the fact of inaccuracy of Personal Data or the illegality of their processing is confirmed, the Personal Data must be updated by the Operator, or their processing must be stopped accordingly. Data protection Officer should be notified (24/7) as per SOP06/BP.

Если факт неточности предоставленных персональных данных или незаконности их обработки подтверждается, то такие персональные данные должны быть обновлены Оператором или их обработка должна быть прекращена надлежащим образом. Должностное лицо по защите персональных данных должен быть уведомлен (24/7) в соответствии с SOP06/BP.

5.5.2 The fact of inaccuracy of Personal Data or illegality of their processing can be established either by the Data Subject or by the NCA.

Факт недостоверности персональных данных или незаконности их обработки может быть установлен либо Субъектом, либо НПО.

5.5.3 At the written request of the Data Subject or his/her representative, the Operator is obliged to provide information about the processing of Personal Data of the specified subject by him. The request must contain the number of the main document identifying the Data Subject and his/her representative, information about the date of issue of the specified document and the issuing authority, information confirming the participation of the Data Subject in relations with the Operator (without limitation):

По письменному запросу Субъекта или его представителя Оператор обязан предоставить информацию об обработке им персональных данных указанного Субъекта. Запрос должен содержать номер основного документа, удостоверяющего личность Субъекта и его представителя, информацию о дате выдачи указанного документа и органе, выдавшем его, информацию, подтверждающую участие Субъекта в отношениях с Оператором (без ограничений).

- contract number / контактный номер,
- date of conclusion of the contract / дата заключения договора,
- conventional verbal designation and (or) other information) / текстовое содержание коммуникации и (или) другая информация,
- or information otherwise confirming the fact of processing of Personal Data by the Operator / или информация, иным образом подтверждающая факт обработки персональных данных Оператором,
- signature of the Data Subject or his/her representative / подпись Субъекта или его представителя.

The request can be sent in the form of an electronic document and signed with an electronic signature in accordance with the local law.

Запрос может быть отправлен в электронном виде и подписан электронной подписью в соответствии с локальным законодательством.

5.5.4 If the request of the Data Subject does not reflect all the necessary information or the subject does not have access rights to the requested information, then a reasoned refusal is sent to him.

Если в запросе Субъекта отражена не вся необходимая информация или Субъект не имеет прав доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

5.5.5 In the manner provided for in clause 5.5.3, the Data Subject has the right to demand that the Operator clarify his/her personal data, block it or destroy it if the personal data is incomplete, outdated, inaccurate, illegally obtained or is not necessary for the stated purpose of processing, as well as take measures provided by law to protect the rights.

В порядке, предусмотренном пунктом 5.5.3, Субъект имеет право потребовать от Оператора уточнения его персональных данных, заблокировать их или уничтожить, если персональные данные являются неполными, устаревшими, неточными, получены незаконным путем или не являются необходимыми для заявленной цели обработки; а также принять меры, предусмотренные законом для защиты этих прав.

5.5.6 When the objectives of processing Personal Data are achieved, as well as in the case that the Data Subject withdraws Consent, Personal Data is subject to destruction if:

При достижении целей обработки персональных данных, а также в случае отзыва Согласия Субъектом, персональные данные подлежат уничтожению, если:

- the Operator has no right to carry out processing without the Consent of the Data Subject.
Оператор не имеет права осуществлять обработку Субъекта без его согласия.
- otherwise is not provided for by the agreement to which the Data Subject is a party, beneficiary or guarantor.
иное не предусмотрено соглашением, стороной, выгодоприобретателем или гарантом которого является Субъект персональных данных.
- otherwise is not provided for in another agreement between the Operator and the Data Subject.
иное не предусмотрено в рамках другого соглашения между Оператором и Субъектом персональных данных.

VI. RESPONSIBILITIES / ОТВЕТСТВЕННОСТЬ

All employees of ZM CRO GROUP® are responsible for maintaining the confidentiality of the Personal Data in accordance with this Policy, SOP06/BP, CDA and global and local laws.

Все сотрудники ZM CRO GROUP® несут ответственность за поддержание конфиденциальности персональных данных в соответствии с положениями данной Политики, SOP06/BP, СОД, глобальным и локальным законодательством.

Third parties, including contractors and consultants, are required to sign CDA and DPA and abide by this Policy.

Третьи стороны, включая поставщиков услуг и консультантов обязаны подписать СОК и СОД и ознакомиться с данной Политикой.

VII. FORMS / ФОРМЫ

Not applicable / Не применимо

VIII. REFERENCES / ССЫЛКИ

SOP03/BP – Record management and security / Безопасность и управление записями.

SOP02/IT – Electronic Information Security / Безопасность электронной информации.

SOP06/BP – Personal Data Protection / Защита персональных данных.

IX. REVISION AND REVIEW HISTORY / ИСТОРИЯ ПРОСМОТРА И ИЗМЕНЕНИЙ

VERSION Версия	REASON FOR ISSUE OR REVIEW Причина для публикации или пересмотра	ISSUE DATE Дата публикации
1.0	Initial issue of Policy	01-Mar-2024
n/a не применимо	Translated in Russian. Переведено на русский язык	06-Feb-2026 / 06-Фев-2026