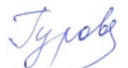




ZM CRO GROUP POLICY

TITLE:	Confidentiality Policy
INDEX CODE:	BP06-POL-19
VERSION NUMBER:	1.0
EFFECTIVE DATE:	01-Mar-2024
DUE DATE FOR SCHEDULED REVISION:	01-MAR-2026

SIGNATORIES

ROLE	NAME, TITLE	SIGNATURE	DATE
AUTHOR	Elena Gurova, Development Director, Quality Assurance Manager of ZM CRO GROUP®		29-Feb-2024
REVIEWER	Yuri Zaretsky, CEO of ZM CRO GROUP®		29-Feb-2024
APPROVER	Yuri Zaretsky, CEO of ZM CRO GROUP®		29-Feb-2024

I. PURPOSE

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.

II. SPHERE OF APPLICATION

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.

III. DEFINITIONS

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

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.

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.

Contingent worker – employee who is hired 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.

Data operator / processor¹ – 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.

¹ 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.

Data subject – any natural person, whose personal data is being processed, e.g. employee, research subject, investigator, representative of the sponsor or any other natural person.

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

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.

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.

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.

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.

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.

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, sexual life or offences or alleged criminal offences.

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.

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

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

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

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;

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.

MAH – Marketing Authorization Holder.

CRO – Contract Research Organization.

CDA – Confidentiality and Disclosure Agreement.

DPA – Data Processing Agreement.

NCA – National Regulatory Authorities.

IV. POLICY

A. Rights and obligation of Data Controller

Data Controller is obliged to:

- determinate the purposes and means of processing Personal Data.

Data Controller is obliged to:

- take into account the purpose, nature, context, and scope of any data processing activities.
- consider the likelihood of any severe risk to the freedoms and rights of any natural persons.
- implement appropriate organizational and technical measures and security measures that demonstrate that the data processing activities have been performed in accordance with local regulations.
- review and update these measures where necessary.
- notify the competent supervisory authority of any breach likely to endanger individuals' rights and freedoms without undue delay.
- appoint a Data Protection Officer, when necessary.
- perform data protection impact assessment.

B. Rights and obligation of Data Operator / Processor

The Operator/Processor has the right to:

- receive reliable information and/or documents containing Personal Data from the Data Subject.
- require the Data Subject to clarify the provided personal data in a timely manner.

- 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.

The Operator/Processor is obliged to:

- process Personal Data in accordance with the procedures established by the current legislation (global and/or local).
- consider the requests of the Data Subject regarding the processing of Personal Data and provide motivated answers.
- provide the Data Subject with the possibility of free access to his/her Personal Data.
- 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.
- organize the protection of Personal Data in accordance with the requirements of the current legislation (global and/or local).
- assist the Data Controller in fulfilling their obligations under the law.
- appoint a Data Protection Officer, when necessary.
- notify the Data Controller of any breach likely to endanger individuals' rights and freedoms without undue delay.
- ensure that international transfers of Personal Data are comply with the local law.
- publish or provide otherwise unrestricted access to this Policy.

C. Rights and obligation of Data Subjects

Data Subjects have the right to:

- obtain a full information about their Personal Data processed by the Operator/Controller.
- 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.
- 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.
- withdraw consent to the processing of Personal Data.
- take legal measures to protect their rights.
- exercise other rights in accordance with local laws.

Data Subjects are obliged to:

- provide the Operator/Controller with only reliable information about yourself.
- provide documents containing Personal Data to the extent necessary for the purpose of processing.
- inform the Operator/Controller about the clarification (updating, modification, etc.) of their Personal Data.

V. GUIDELINES and PROCEDURES

5.1 Scope and categories of Personal Data processed, categories of Data Subjects:

5.1.1 Scope of Personal Data processed:

- 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).
- Personal Data from Clinical trial²** (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).
- 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 reaction / incident (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)).

5.1.2 Categories of Data Subjects:

- Staff (e.g. employees, consultants, temporary workers, etc.).
- Business partners (e.g., manufacturers, distributors, medical representative, etc.), clients and vendors.
- Consumers (e.g. patients, healthcare professionals, etc.).
- Regulatory Authorities.

5.2 Purposes of Personal Data collection:

- maintaining personnel and accounting records, registration of labor and civil relations.

² 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.

- 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.
- implementation of other functions, powers and obligations assigned to the Operator/Processor.

5.3 Legal basis for the processing of Personal Data:

- Good pharmacovigilance practice.
- Good clinical practice.
- GDPR.
- GCDMP.
- Labore codes.
- Local data protection regulatory requirements and guidelines.
- Agreements concluded between the Operator and Data Subject.
- Consent of personal data subjects to the processing of Personal Data.
- Other grounds when consent to the processing of Personal Data is not required by law.

5.4 Procedures and conditions of Personal Data processing:

5.4.1 The processing of Personal Data by the Operator is carried out in the following ways:

- without using automation tools;
- in information systems with or without transmission of the received information via information and telecommunication networks;
- mixed processing of Personal Data.

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.

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.

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.

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.

5.4.5.1 These measures shall include as appropriate (without limitations):

- the pseudonymization and encryption of Personal Data.
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident.
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

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.

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

5.5 Updating, correction, removal and destruction of Personal Data, responding to requests for access to Personal Data by Data Subjects:

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.

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.

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):

- contract number,
- date of conclusion of the contract,
- conventional verbal designation and (or) other information),
- or information otherwise confirming the fact of processing of Personal Data by the Operator,
- signature of the Data Subject or his/her representative.

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

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.

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.

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:

- the Operator has no right to carry out processing without the Consent of the Data Subject.
- otherwise is not provided for by the agreement to which the Data Subject is a party, beneficiary or guarantor.
- otherwise is not provided for in another agreement between the Operator and the Data Subject.

VI. RESPONSIBILITIES

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.

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

VII. FORMS

Not applicable.

VIII. REFERENCES

SOP03/BP – Record management and security.

SOP02/IT – Electronic Information Security.

SOP06/BP – Personal Data Protection.

IX. REVISION AND REVIEW HISTORY

VERSION	REASON FOR ISSUE OR REVIEW	ISSUE DATE
1.0	Initial issue of Policy	01-Mar-2024