

POLICY FOR THE PROCESSING OF PERSONAL DATA IN BB-NCIPD EAD

This Policy for the processing of personal data has been prepared and adopted by the Management of BB-NCIPD EAD in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46/EC (General Data Protection Regulation - GDPR).

The GDPR entered into force on the twentieth day after its publication in the Official Journal of the European Union and is mandatory in its entirety, applying directly in all Member States from 25 May 2018, according to Article 99 of the GDPR.

This Privacy Policy applies to personal data collected through the website, as well as to the provision of products produced by BB-NCIPD EAD.

The purpose of this policy is for natural persons to be informed what personal data is collected about them, for what purpose, term and what their rights are.

BB-NCIPD EAD attaches great importance to the protection of personal data and undertakes to comply with the current legislation on the protection of personal data. BB-NCIPD EAD will observe the highest levels of confidentiality of personal data.

This Policy for the protection of personal data of natural persons has been adopted by BB-NCIPD EAD.

All persons who have legal or factual relations with BB-NCIPD EAD and/or access to the personal data processed by it must familiarize themselves with and comply with this policy. Agreeing with it is a condition for entering into and realizing legal relations with BB-NCIPD EAD. If you do not agree with this policy, you will not be able to enter into legal relations with BB-NCIPD EAD.

Access to processed personal data is granted only in cases defined by law to entitled persons on the basis of a valid legal basis and/or a previously concluded data confidentiality agreement with persons who provide sufficient guarantees for the application of appropriate technical and organizational measures in such a way that the processing takes place in accordance with the requirements of the GDPR and ensures the protection of the rights of the data subjects and who have undertaken an obligation to observe confidentiality. BB-NCIPD EAD carries out inspections of compliance with the obligations assumed by the agreement.

In accordance with the GDPR, other relevant documents, policies, practices, processes and procedures are described and adopted in this policy.

Administrator data:

BB-NCIPD EAD, UIC 207939249 is a company specialized in the production and sale in the country and abroad of vaccines, serums, allergens, blood products, immunostimulants, diagnostic preparations and other preparations for diagnosis, treatment and prevention.

Contact details:

Country: Bulgaria

Address: BB-NCIPD EAD, UIC 207939249, with registered office and management address:
1504 Sofia, 26 Yanko Sakazov Blvd.

Telephone: +3592 9446999

Fax: +3592 9443455

E-mail: gdpr@bulbio.com

Internet address: <http://www.bulbio.com/>

Data Protection Officer contact details:

Our Data Protection Officer can be contacted at:

Maria Georgieva Nestorova

E-mail: gdpr@bulbio.com; maria.nestorova@suis.bg

Telephone: +359 882 727 270

For the purposes of its activity as a commercial company, BB-NCIPD EAD processes personal data of natural persons ("data subjects") in strict accordance with the GDPR, the Personal Data Protection Act and this Personal Data Processing Policy.

According to GDPR and this policy:

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;;

"Restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future;

"Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;;

"Pseudonymization" means 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, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

"Processor of personal data" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

"Recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

"Third party" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

"Personal data register" means any structured set of personal data that is accessed according to certain criteria, whether centralized, decentralized or distributed according to a functional or geographical principle;

"Consent of the data subject" means 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;

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"Genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

"Biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

"Health data" means 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.

When processing personal data, BB-NCIPD EAD observes and is guided by the principles laid down in the GDPR for: legality; good faith and transparency; limitation of objectives; data minimization; accuracy; storage limitation; integrity and confidentiality.

Information and personal data that BB-NCIPD EAD collects

When you use our website's adverse drug reaction (ADR) reporting form, inquiry form or select the products we offer, we collect information and personal data about you, which in most cases you provide us yourself, choosing and agreeing to submit information about yourself. In certain cases, we require your personal data to comply with a legal obligation, to enter into a contract with you, to take steps at your request prior to entering into a contract, to protect your or another individual's vital interests, to perform a task in the public interest or in the exercise of official powers granted to us, for the purposes of our legitimate interests or those of a third party, except where your interests or fundamental rights and freedoms that require the protection of personal data take precedence over such interests, more especially when the data subject is a child.

Depending on the relationship you wish us to enter into, we may collect and process the following information about you: name, personal identification number, identity card data, gender, address, age/date of birth, contact telephone number, e-mail address, educational and qualification degree, additional qualification and legal capacity, specialty, etc. In the event that we need to collect special categories of personal data (health data, etc.), they are used for the needs of drug safety and in the presence of any of the conditions listed in the GDPR:

- In the presence of the person's express consent to the processing for one or more specific purposes, unless the legislation excludes the possibility of such consent;
- For the purposes of preventive or occupational medicine, to assess the working capacity of employees, the provision of health or social care;
- In order to protect vital interests of the data subject or another natural person, where the data subject is physically or legally unable to give consent;
- To protect the public interest in the field of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and medicinal products or medical devices;
- For the purposes of fulfilling the obligations and exercising the special rights of the administrator or the data subject under labor law and social security and social protection law, insofar as this is permitted by the Union law or the law of a Member State, or pursuant to a collective agreement in accordance with the law of a Member State, which provides for appropriate safeguards for the fundamental rights and interests of the data subject;
- For reasons of important public interest, on the basis of the Union law or the law of a Member State, which is proportionate to the objective pursued, respects the essence of the right to data protection and provides for appropriate and specific measures to protect the fundamental rights and interests of the data subject.

In view of their sensitive nature, the special categories of personal data enjoy enhanced protection and are processed by specialists from the company in compliance with the obligation of professional secrecy.

The listed data is collected by:

- Users of the company's products, medical persons;
- Personnel, current and former employees of the company, job candidates and trainees;
- Contractors or potential contractors of the company and/or their employees.

BB-NCIPD EAD processes personal data for the following purposes:

(a) Production and sale in the country and abroad of vaccines, serums, allergens, blood products, immunostimulants, diagnostic preparations and other preparations for diagnosis, treatment and prevention.

With regard to the services available on the website of BB-NCIPD EAD and the online registration forms in connection with submission of requests, ADR reporting, responses to your inquiries, complaints or other correspondence.

(b) Fulfillment of the company's legal obligations, regulated in Regulation (EC) No 726/2004 of the European Parliament and of the Council of 31 March 2004 to establish Community procedures for the authorization and control of medicinal products for human and veterinary use and to create European Drug Agency, the Medicinal Products in Human Medicine Act (MPHMA), the Health Act, the Health Insurance Act, the Medical Institutions Act, the Consumer Protection Act, the issued by-laws on their implementation, for the

needs of state control over medicinal products, provision of information to the Minister of Health, the Chief State Health Inspector, the Executive Director of the Bulgarian Drug Agency (BDA), for the needs of the European Pharmacopoeia, the Pharmacopoeia Committee, the Supreme Council of Pharmacy, the Bulgarian Pharmaceutical Union, the National Health Insurance Fund (NHIF), to monitor the safety of medicinal products placed on the market, the preparation of a positive medicinal list, the control of production and import, wholesale and retail trade, the conduct of clinical trials, advertising and the system for monitoring the safety of medicinal products placed on the market, the principles and requirements for good manufacturing practice (GMP) of all types of medicinal products, etc.;

- (c) Fulfillment of the requirements of labor, insurance and social legislation in relation to employees;
- (d) Fulfillment of obligations regulated in accounting and tax legislation;
- (e) Guaranteeing the security of visitors, employees and property through video surveillance, registration, physical security and access control;
- (f) Other lawful purposes related to the physical and informational security of the website and IT systems and protection of the legitimate interests of BB-NCIPD EAD;
- (g) Performance of a contract, including pre-contractual relations before its conclusion.

Provision of personal data

BB-NCIPD EAD provides personal data to competent state authorities in fulfillment of their legal obligations, including, but not limited to: The Minister of Health, the Chief State Health Inspector, the Executive Director of the BDA, the Pharmacopoeia Committee, the Higher Council of Pharmacy, the Bulgarian Pharmaceutical Union, the National Health Insurance Fund, the National Revenue Agency, the National Social Security Institute, and others.

BB-NCIPD EAD uses third parties to support certain activities such as: external laboratories or medical facilities; external consultations with specialists, commercial companies providing services to the Company, including information maintenance and security of IT systems, accounting, hosting and maintenance of the website and communications and others.

In view of the fact that the GDPR provides guidelines for the administrator of personal data to outsource the processing of personal data only to persons who have a reason to receive them and provide sufficient guarantees for the implementation of appropriate technical and organizational measures in such a way that they meet to the requirements of the regulation: in all these cases BB-NCIPD EAD will take the necessary measures to protect the rights and interests of the personal data subjects, based on the express contracts concluded with the processors of personal data to guarantee the security of the data and protect their confidentiality, which regulate the subject and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects and the duties and rights of the administrator according to Article 28 of the GDPR.

BB-NCIPD EAD will not transfer personal data to third countries outside the European Union, except when necessary for the purposes of commercial relations with third countries (issuance of certificates, commercial contracts, licenses and others). In these cases, with a view to protecting the rights and interests of the data subject, express prior consent to the data transfer is requested. Personal data may be protected in other ways, for example by signing a contract between the company and the recipient, including standard clauses for the protection of personal data adopted by the European Commission.

Terms of storage of personal data

The information collected for you is stored until the end of the relationship with the company or according to the terms provided for in the current legislation, including according to Ordinance No 15 of 17.04.2009 on the conditions for issuing a production/import permit and the principles and requirements for good manufacturing practice of all types of medicinal products, of medicinal products for clinical trials and of active substances and for the storage of the documentation for each concluded transaction for a medicinal product (documentation for the purchases and/or sales of all medicinal products).

The personal data of natural persons are stored in accordance with the legally defined deadlines for the relevant clinical trials and the principles and requirements for good manufacturing practice (GMP) of all types of medicinal products.

The personal data of job applicants who are not approved for appointment in the company are stored for the period determined according to the current regulations in the field of personal data protection, from the end of the procedure, after which they are returned to the person or destroyed. Personal data can be

stored for a longer period, for the purpose of making job offers, only with the applicant's written consent.

The personal data of the employees at BB-NCIPD EAD are stored within the time limits according to the current labor legislation.

Video surveillance recordings are stored for a period of 60 (sixty) days in accordance with the Law on Private Security Activities.

Personal data contained in accounting documents are stored within the terms of Article 12 of the Law on Accounting.

Security of personal data

BB-NCIPD EAD implements all appropriate technical and organizational measures to guarantee the security of personal data, including taking on an express obligation by employees for professional secrecy and confidentiality.

BB-NCIPD EAD processes personal data in a way that guarantees an appropriate level of their security, including protection against unauthorized or illegal processing and against accidental loss, destruction or damage, applying appropriate technical or organizational measures. The Company has implemented and maintains an information security management system in accordance with the requirements of the international standard ISO/IEC 27001:2022.

In accordance with Recital 49 of the GDPR, the processing of personal data to the extent that is strictly necessary and proportionate to the objectives of ensuring network and information security, i.e. the ability of a given network or information system to withstand, with an appropriate level of confidence, random events or illegal or malicious actions that affect the availability, authenticity, integrity and confidentiality of personal data stored or transmitted, as well as the security of related services, offered or accessible through these networks and systems, by public authorities, computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), providers of electronic communications networks and services, and technology providers and security services, is a legitimate interest of the relevant data administrator. This may include, for example, preventing unauthorized access to electronic communications networks and the spread of malware, and stopping denial-of-service attacks and damage to computers and electronic communications systems.

BB-NCIPD EAD takes measures to guarantee the security of the processing considering:

- the achievements of technical progress, the costs of implementation and the nature, scope, context and purposes of processing, as well as risks of varying probability and severity for the rights and freedoms of natural persons, the administrator and the processor of personal data apply appropriate technical and organizational measures to ensure a tailored with that risk level of security including, inter alia, where appropriate:
 - pseudonymization and encryption of personal data;
 - ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - ability to promptly restore availability and access to personal data in the event of a physical or technical incident;
 - a process of regular testing, assessment and evaluation of the effectiveness of technical and organizational measures in order to guarantee the security of the processing.

In the event of a breach of personal data security, BB-NCIPD EAD will notify the supervisory authority of the breach of personal data security without undue delay and when feasible - no later than 72 hours after becoming aware for it.

Rights of data subjects

GDPR regulates in detail the rights of the data subject (Article 12 et seq.).

Every natural person whose data is processed by BB-NCIPD EAD has the following rights: right to transparent information, communication and conditions for the exercise of the data subject's rights, right to information provided when collecting personal data from the data subject and access to it, right to correction, right to correction and deletion of personal data (right "to be forgotten"), right to restriction of processing, right to receive and portability of personal data, right that is correlative to the administrator's obligation to notify upon correction or deletion of personal data or restriction of processing, right to object to the processing of personal data, the right of the data subject not to be subject to a decision based solely on automated processing, including profiling, which gives rise to legal consequences for the data subject or

similarly affects him/her to a significant extent, the right of defense before competent authorities.

The right of access to information of the participants in a clinical trial and the provision of information, including in connection with the monitoring of safety and/or serious adverse drug reactions, is exercised according to the order of LMPHM.

Information may be provided to third parties under the conditions and in accordance with the provisions of the LMPHM.

Online protection when completing an adverse drug reaction (ADR) reporting form.

In accordance with the Personal Data Protection Act, the above rights can be exercised by submitting a written application to: 1504 Sofia, 26 Yanko Sakazov Blvd., "Information Security" unit. An application can also be submitted electronically, in accordance with the Law on Electronic Documents and Electronic Authentication Services.

The application is made personally by the data subject or by a person expressly authorized by him/her with a notarized power of attorney, a copy of which is provided with the application.

A response to a request for an exercised right is prepared on paper and is received by the applicant at the address of BB-NCIPD EAD at the Company's Registry Office. Employees of the "Information Security" unit verify the identity of the applicant by reference to an identity document presented by the latter and provide the answer in two copies, one for each party, signed by the applicant.

All natural persons - data subjects have the right to access their personal data stored by BB-NCIPD EAD, as well as the right to correct and supplement such data. All requests for access, correction, blocking and/or deletion of personal data should be sent to the Personal Data Administrator at the following addresses:

1504 Sofia, 26 Yanko Sakazov Blvd., "Information Security" unit

Telephone: +359 2 944 69 99

Fax: +359 2 943 34 55

E-mail: gdpr@bulbio.com

The personal data administrator sends the sender a confirmation of receipt within 5 working days after receiving the request and a specific motivated response to the request within 20 calendar days. When this is not possible, the sender is notified of the next steps and the reasons for the delay. In this case, the final response of the Personal Data Administrator should be sent to the sender within 60 calendar days.

In case of irregularities or obvious misuse by the data subject in exercising his/her rights, the Personal Data Administrator may consult the data protection officer regarding the request and/or refer the data subject to the data protection officer, to decide on the admissibility of the request and the appropriate follow-up.

Protection of data subjects' rights

In accordance with the GDPR and the Personal Data Protection Act, any natural person who believes that his/her right to the protection of his/her personal data has been violated may submit a complaint to the Personal Data Protection Commission at the address: 1504 1595 Sofia, 2 Prof. Tsvetan Lazarov Blvd., website: www.cdpd.bg.

This Personal Data Protection Policy is in accordance with current legislation and is subject to annual review for up-to-dateness.

26.08.2024

**Executive Director:
Dr. Roumen Kofinov**