

**CONFIDENTIALITY POLICY OF THE COMPANIES IN THE GROUP OF
ACIBADEM CITY CLINIC IN COMPLIANCE WITH REGULATION (EU) 2016/679
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

Contents

1. DEFINITIONS.....	1
2. SUBJECT MATTER AND SCOPE.....	2
3. CATEGORIES OF DATA SUBJECTS AND CATEGORIES OF PERSONAL DATA.....	3
4. PURPOSE AND LEGAL GROUNDS TO PROCESS PERSONAL DATA IN THE GROUP	5
5. RECIPIENTS AND CATEGORIES OF RECIPIENTS OF PERSONAL DATA	7
6. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OUT OF EU AND EEA ...	8
7. TIME LIMITS FOR STORAGE OF PERSONAL DATA IN THE GROUP	8
8. RIGHTS OF DATA SUBJECTS	9
9. RIGHT TO COMPLAIN TO A SUPERVISORY AUTHORITY	9
10. MEASURES FOR PERSONAL DATA PROTECTION.....	9
11. DATA PROTECTION OFFICER IN THE GROUP	10

1. DEFINITIONS

The definitions specified below have been implemented in line with Regulation (EU) 2016/679:

“Personal Data” means any information related to an identified natural person or a natural person who can be directly or indirectly identified by using an identifier (*data subject*).

“Special Category of Personal Data” means any personal data disclosing racial or ethnic background, political views, religious or philosophical beliefs or membership in syndicates, as well as processing of genetic data, biometric data only for the purpose of identification of a natural person, details about the health status or details about the sexual life or sexual orientation of the respective 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;

“Data Subject” means any natural person whose personal data is processed within the Group.

“**Controller**” means a company within the Group which, on its own or together with other companies within the Group, specifies the purpose and media of personal data processing. When the purpose and the media of such processing is governed by the law in EU or the law in the member-state, the controller or the special criteria for its definition may be set out in the law in EU or in the law of a member-state.

“**Personal Data Processor**” means any natural person or legal entity, public authority, agency or another structure that processes personal data on behalf of the controller.

“**Third Party**” means any natural person or legal entity, public authority, agency or another authority which is different from the data subject, controller processing personal data and persons who are directly supervised by the controller or the personal data processor have the right to process the personal data.

“**Violation of Personal Data Security**” means a violation in the security which brings to accidental or unlawful deletion, loss, change, non-permitted disclosure or access to personal data which is transferred, stored or processed in another way.

“**Group of Enterprises**” means a controlling enterprise and the enterprises controlled by it specified in the “**Group**” under Recital 37 of Regulation (EU) 2016/679.

“**The Group**” means companies doing commercial activity in the Republic of Bulgaria as specified in Appendix No. 1.

“**Hospitals**” means companies in the Group that render medical services in line with the Hospital Act.

“**Supervisory Authority**” means Personal Data Protection Committee in the Republic of Bulgaria.

2. SUBJECT MATTER AND SCOPE

ACIBADEM CITY CLINIC EAD, headquartered at: Sofia, 53 Nikola Y. Vaptsarov blvd., floor 4, tel/fax: +359 2 960 4929, is a Bulgarian legal entity whose sole owner is Acibadem City Clinic B.V., headquartered and registered address at: the Netherlands, 1034KE, Amsterdam, 36 Coopvaardersplantsoen.

This policy is applied at ACIBADEM CITY CLINIC EAD, which, together with its subsidiaries (as specified in Appendix No. 1) make up the group of the Bulgarian enterprises Acibadem City Clinic (**the/Group**).

The purpose of this policy is to give clear and complete information to the subjects about the approved personal data protection standards that the Group applies in line with the provisions of Regulation (EU) 2016/679 (**The/Regulation**) and the applicable law in Bulgaria.

All the companies in the Group are controllers of personal data and process personal data in compliance with the provisions of the Regulation and the valid legislation in Bulgaria.

The policy shall apply when collecting, processing and sharing personal data for internal administrative purposes among the companies and the Group.

Together with this Policy, each of the companies in the Group has adopted its confidentiality policy. This policy gives information to the subjects about specific conditions under which

their personal data is processed in line with the subject matter of the activities of those companies.

3. CATEGORIES OF DATA SUBJECTS AND CATEGORIES OF PERSONAL DATA

3.1. Patients and their families/friends

The Group collects personal data directly from patients when offering healthcare/medical services, as well as for administrative and internal business purposes, including for legal interests related to the presence/stay/treatment of a patient within the hospitals in the Group.

When rendering healthcare/medical services, the hospitals in the Group may collect the following categories of personal data:

- *Regular personal data*: names, ID No., passport details, address, place of birth, telephone number, email, gender, number of an insurance policy, financial information, other relevant information related to rendering healthcare/medical services;
- *Special personal data*: health condition, genetic data, and when relatable, information about sexual life and sexual orientation. Such data is usually included in medical documentation (medical reports, outpatient cards, other documents, part of the patient's file, laboratory results, consultations and expert's notes, prescriptions of prescribed treatment regime, radiology results and examinations, etc.)

In case of emergency and urgent situations, personal data about the patient can be collected from their family and friends.

In some cases, a hospital in the Group may participate in clinical research. In such cases, if the data subject is invited to take part in clinical research, he/she will get preliminary information about the nature and specifics of the research, as well as what kind of personal data is needed to conduct it.

If a company in the Group decides to process data of subjects for marketing purposes, it shall take the necessary measures to obtain the informed consent of the data subject beforehand.

3.2. Applicants for work

- *Regular personal data*: information in the candidate's CV (Curriculum Vitae), such as names, contact details (telephone number and email), copy of documents for professional and educational qualifications, etc.

When needed, in terms of legal requirements to medical and other specialists who apply for a vacancy, it is possible to request additional information from the respective person, including sensitive personal data. The company shall inform the respective person about the specific legal ground pursuant to which the information should be submitted as well as the consequences from its non-submission.

3.3. Staff

The companies in the Group collect the following categories of personal data from the employees:

- *Regular personal data*: names, ID No., passport details, education and qualifications, profession, experience, remuneration, bank account details and other;
- *Special personal data*: information about health condition included in hospital charts, documents proving long-term incapacity to work and/or other documents needed under the applicable legislation for the respective position or in line with the application of certain rights of the employee.

In general, the Group does not process personal data of employees based on consent. Yet, it is possible, in certain cases, the consent to be needed when it is required under the applicable law, incl. processing of special category of personal data.

3.4. CCTV and Call Center

In some premises that are owned or managed by a company in the Group there are installed CCTV systems; as a result CCTV records (video images) of data subjects (visitors and/or patients) are kept. In such cases the data subjects are informed that CCTV has been recording via information signs placed at visible spots on the sites and premises.

The companies in the Group have a unified call center; patients can book an appointment for a check-up or consultation with the respective specialist beforehand through it. Incoming and outgoing calls made through the call center are recorded; so, in this way, through the audiorecords the following personal data can be collected – the names of a persona and telephone number.

More detailed information about the conditions under which video- and audio-records are recorded and the time limit for their storage can be found in the Confidentiality Policy of the respective company in the Group.

3.5. Internet users

The main webpage <https://www.acibademcityclinic.bg/> of the Group and the webpages linked to it with the location of the hospitals use “cookies”. Therefore, when users access them, the following data might be collected: type of operating system, supplier of internet services and others. For further information, please, see the respective Cookies Policy.

Each webpage of a Group hospital contains a contact form. When completing the contact form, the user gives the following information: first and last names, telephone, email.

Besides the contact forms, the webpages of the hospitals in the Group have a section titled “Careers” where vacancy information is regularly posted. The users who want to apply for should send their CV to the email indicated for that purpose; in this way they give the personal data in it.

Further, on the webpages, in the section “About Us” and its subsections, information, materials and news are posted as they might contain personal data for the employees in the respective hospital in the Group, such as: names, position, image or other related information.

In addition, letters of gratitude by patients are posted in the section “*The Patients about Us*”. Because of the descriptive nature those letters might have, they may contain personal data which is blacked out before posting.

3.6. Applicants/claimants/appellants/plaintiffs

To protect their legal interests, the controllers of the Group process the following categories of personal data:

- *Regular personal data*: names, ID No., passport details, email, address and other details specified in the complaints, applications, claims, fines, penal decrees, etc.;
- *Special personal data*: information about health condition.

3.7. Business partners, clients and suppliers

The Group processes personal data of natural persons who represent (lawfully or by means of a letter of authorization) or work as business partners, suppliers and investors of the Group. Because of that and as much as it is admissible during regular commercial activities, the Group may process the following categories of personal data:

- *Regular personal data*: names, address, telephone, email and other details that are relatable to the specific case.

4. PURPOSE AND LEGAL GROUNDS TO PROCESS PERSONAL DATA IN THE GROUP

4.1. Patients and their family/friends

The hospital in the Group process personal data for the health status of the patients by strictly observing the provisions of Regulation (EU) 2016/679 and the applicable legislation as far as this processing is needed for the purposes of medical diagnosis, to provide healthcare and social cares and treatment to patients, as well as it is needed for the purposes of preventive and occupational medicine, for the assessment of the work capability of an employee.

In addition, some of the following alternative justifiable reasons are applied to the specific case:

- The processing is needed to protect vitally important interests of the data subject or another natural person when the data subject is physically or legally incapable of giving their consent;
- The processing is needed because of public interest in the sphere of public health such as protection against serious trans-border threats to health or guarantee of high quality and safety standards of healthcare services and drugs or medical consumables;
- The data subject in some cases has given his/her express consent on processing his/her personal data for one or more specific purposes unless the right in the Union and the right of a member-state does not exclude the possibility for such a consent by the data subject.

4.2. Applicants for work

The companies in the Group process personal data of candidates for work for the purposes of staff selection on the following grounds:

- Taking steps upon the request of a data subject before the execution of a contract;

- The processing is needed for the purposes of legitimate interests of the respective company unless the interests and fundamental rights and freedom of the data subject does not prevail over such interests;
- Prior given explicit consent by the data subject.

4.3. Staff

In general, the companies of the Group process data of the staff when:

- The processing is needed for the implementation of the contract under which the data subject is a party or for taking steps upon the request of the data subject before the execution of the contract;
- The processing is needed to abide by the legal obligation imposed to a company in the Group, more specifically in relation to the employment and social laws;
- The processing is needed for the legitimate interests of the respective company in the Group unless the interests and fundamental rights and freedom of the data subject does not prevail over such interests;
- As an exception, personal data can be processed pursuant to the consent by the data subject for one or more specific purposes (for example, marketing);

The companies in the Group may process special categories of personal data of its employees/workers – details about their health condition when such processing is needed for the purposes of the employment law and the laws in the sphere of social security and social protection in line with the applicable national legislation.

Personal data in regard to verdicts and violations (specified in criminal record certificates) about employees is collected and processed by the respective company in the Group only if that is indicated in a regulatory document.

4.4. CCTV and Call Center

CCTV data is processed for:

- Protection of the legitimate interests of the respective company in the Group;
- When the processing is needed to protect vitally important interests of the data subject or of another natural person.

In certain cases, CCTV records might be made due to a regulatory obligation that the respective company in the Group has in regard to specific premises on the site.

The audio-records of phone calls made at the call center of the hospitals in the Group (together with the personal data they contain) are collected and processed for the legitimate interests of the respective company in the Group unless the interests and fundamental rights and freedom of the data subject does not prevail over such interests.

The personal data of staff published in the section “About Us” on the webpage of the respective hospital in the Group is processed after the prior consent of the data subject.

The Group processes personal data included in letters of gratitude by patients and published in the section “Patients about Us” for its legitimate interest when popularizing and building up trust in the quality of the offered healthcare/medical services by the respective hospital.

4.5. Applicants/claimants/appellants/plaintiffs

The Group processes personal data of those categories of subjects only as much as needed for the protection of its legitimate interests, as well as for exercising or protection of legal claims against the controller . In some cases, the data is processed for the implementation of a regulatory obligation of the controller.

4.6. Business partners, clients and suppliers

The Group processes data about business partners, clients and suppliers as much as it is needed for the implementation of the contract under which the data subject is a party or for taking measures upon the request of the data subject before the execution of the contract. In other cases, the processing of that personal data might be needed for the protection of the legitimate interest of the controller from the Group or for the implementation of the legal obligations of the Group.

5. RECIPIENTS AND CATEGORIES OF RECIPIENTS OF PERSONAL DATA

5.1. In the Group

The processing of personal data might involve data exchange among the companies indicated in Appendix No. 1: List of the Companies in the Group. The Group has a legal interest in such data exchange which is done in order to achieve internal administrative goals, yet, at the same time, the principles of personal data are observed and suitable guarantees are taken for its protection.

5.2. Out of the Group

Personal data may be shared with different categories of recipients. For example, when the controller is implementing its legal obligations, it can submit personal data to the National Revenue Agency, National Social Security Institute, Executive Agency of General Labour Inspectorate, National Health Insurance Fund, Regional Health Insurance Fund, Ministry of Health, Drugs Agency, Executive Agency “Medical Supervision”, Nuclear Regulatory Agency, to competent law enforcement, police authorities, as well as public authorities and institutions.

The group submits data to other natural persons/legal entities that deliver certain type of goods or services to the controller in the Group, including services for information maintenance and security of the IT systems, accounting services, archiving, etc. In such cases, the respective company in the Group enters into a written agreement with the specific service supplier as it has presented sufficient guarantees for the application of suitable technical and organizational measures in such a way so that the processing should run in compliance with the provisions of Regulation (EU) 2016/679 and should guarantee the protection of the rights of data subject.

The group supports partnerships with other independent controllers of personal data – insurance companies, medical universities, hospitals that are out of the Group, physicians with their own practice and others. Regarding those partnerships, the parties might share certain data among themselves, for instance when delivering healthcare/medical services, when acquiring professional or academic qualifications, etc. Then the controllers in the Group shall inform the data subject in a proper manner about those categories of recipients, as well as

about the execution of additional agreements with the respective independent controller so, in this way, they can guarantee the confidentiality of the personal data being shared.

When there are joint controllers among the companies in the Group and a controller out of the Group, then they shall identify in a transparent manner their respective responsibilities for the implementation of the liabilities under Regulation (EU) 2016/679 via an agreement between them.

6. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OUT OF EU AND EEA

Companies in the Group may transfer personal data to countries out of the European Union and European Economic Area only by observing the provisions of Regulation (EU) 2016/679, more specifically, those provisions indicated under Chapter V therein.

The transfer is done pursuant to a decision of the European Commission about the adequate level of protection, which the respective third party provides.

If there is no such a decision by the European Commission, the transfer to a third country might be achieved only if suitable guarantees have been provided and under the condition that there are applicable rights of data subjects and effective legal measures for protection. Suitable guarantees are the adoption of mandatory company rules, standard clauses for protection of personal data, approved code of behaviour or approved certification mechanism.

Alternatively, transfer of personal data to third countries may be done after the express consent of the subject data or when other reasonable grounds are available as specified under art. 49, paragraph 1 of Regulation (EU) 2016/679.

You can find detailed information about the existing transfer of personal data to a third country out of the European Union and European Economic Area in the Confidentiality Policy of the respective controller in the Group.

7. TIME LIMITS FOR STORAGE OF PERSONAL DATA IN THE GROUP

The companies in the Group keep the information they have obtained within the time limits specified as per the legislation and by abiding by the principle of “*restriction of the storage*”, more specifically:

- Personal data of patients is kept in line with the time limits for the respective medical documentation specified in the legislation;
- Personal data of the staff included in the employment documentation shall be kept for 50 (fifty) year pursuant to the National Archive Fund Act, Accounting Act, Social Security Act and Tax-Insurance Proceedings Act;
- Personal data of applicants for work who have not been selected in a company in the Group shall be kept no longer than 6 (six) months after the completion of the procedure; afterwards, it is sent back to the person or destroyed in a proper manner. Personal data might be kept for a longer period in order to offer a work position only if the candidate for work has given their consent for it;
- CCTV records shall be kept for 2 (two) months after making them;
- Audio-records of telephone calls at the call center shall be kept up to 12 (twelve) months and 1 (one) day after making them;

- Personal data available in accounting documents shall be kept in time limits as specified under article 12 of the Accounting Act.

Besides these major time limits, each company in the Group has adopted its policy to identify the time limits for keeping and destruction of the documentation.

8. RIGHTS OF DATA SUBJECTS

8.1. Data subjects have the following rights:

- right to access personal data;
- right to correct or supplement inaccurate or incomplete personal data;
- right to delete personal data;
- right to limit the processing;
- right to personal data portability;
- right to object.

Each company in the Group, depending on the legal grounds upon which personal data is processed, has specified in its policy certain rights that data subjects have and the manner they can exercise them.

Each controller in the Group is independently responsible for the requests received by a data subject.

9. RIGHT TO COMPLAIN TO A SUPERVISORY AUTHORITY

Each data subject, under the circumstances specified in the applicable legislation, may submit a complaint to the Personal Data Protection Commission at address: Sofia, p. box. 1592, 2 Prof. Tsvetan Lazarov blvd.

10. MEASURES FOR PERSONAL DATA PROTECTION

The companies in the Group have already implemented technical and organizational measures for the protection of personal data of natural persons against unlawful access, errors or misuse. The companies in the Group are obliged to observe all the rights of natural persons in connection to the protection of personal data that are guaranteed under the European and national laws.

Each company in the Group has adopted internal rules and procedures of organizational and technical nature, including rules and procedures for identifying the access level that guarantee the confidentiality of the data.

The companies in the Group observe every regulation related to their subject matter of activity by taking into consideration certain circumstances, form of collection of data, legal grounds and the purpose of processing it.

Personal data in the Group is processed solely by the officers expressly authorized to do it and who are informed about their obligations related to the protection of personal data and they have undertaken the commitment of confidentiality.

The premises where personal data is processed and kept have restricted access and are accessible only by the staff processing such data.

The companies in the Group conduct initial and successive trainings to their employees/workers on the policies and procedures for personal data protection.

11. DATA PROTECTION OFFICER IN THE GROUP

Pursuant to art. 37, para. 2 of the Regulation, the Group has appointed a personal data protection officer as this officer is easily accessible by each company.

The data protection officer controls the implementation of this policy applicable in the Group and is a unified contact point for data all subjects in relation to exercising their rights under this Policy and the applicable law on personal data protection.

All the companies in the Group have publicly announced the contact details with the data protection officer in their policies.

The data protection officer is:

Irina Petrova

tel. +359 878 739 296

email: dpo@acibademcityclinic.bg

The data protection officer supports data subjects and he/she is obliged to perform the obligations under art. 37-39 of Regulation (EU) 2016/679 in regard to each of the companies in the Group. A data subject may address all their requests and questions related to exercising their rights under the Regulation to the appointed data protection officer.

This Personal Data Protection Policy has been drawn up and adopted by all the companies in the Group in their capacity of controllers of personal data in terms of performance of their obligations to submit information about data subjects under art. 13 and art. 14 of Regulation (EU) 2016/679 of the European Parliament and of the Council dated 27 April 2016 about the protection of natural persons in regard to the processing of their personal data and to free movement of such data and about the repeal of Directive 95/46/EC (General Data Protection Regulation).

This Personal Data Protection Policy was adopted by the companies in the Group and has been effective since 25 April 2018.

APPENDIX No. 1

LIST OF THE COMPANIES IN THE GROUP OF ACIBADEM CITY CLINIC

1. ACIBADEM CITY CLINIC EAD, at address: Sofia, p.b. 1407, 53 Nikola Vaptsarov blvd., floor 4;
2. ACIBADEM CITY CLINIC - TOKUDA UNIVERSITY HOSPITAL EAD, at address: Sofia, p.b. 1407, 51B Nikola Vaptsarov blvd;
3. ACIBADEM CITY CLINIC – TOKUDA MEDICAL CENTER EAD, at address: Sofia, p.b. 1407, 51B Nikola Vaptsarov blvd.;

4. ACIBADEM CITY CLINIC SERVICES EOOD, at address: Sofia, p.b. 1407, 51B Nikola Vaptsarov blvd.;
5. TOKUDA PHARMACY EOOD, at address: Sofia, p.b. 1407, 51B Nikola Vaptsarov blvd.;
6. CLINICAL RESEARCH CENTER – TOKUDA AD, at address: Sofia, p.b. 1407, 51B Nikola Vaptsarov blvd.;
7. ACIBADEM CITY CLINIC UNIVERSITY HOSPITAL EOOD, at address: Sofia, p.b. 1407, 127 Okolovrasten Pat str. (By-pass road);
8. ACIBADEM CITY CLINIC MEDICAL CENTER EOOD, at address: Sofia, p.b. 1407, 127 Okolovrasten Pat str. (By-pass road);
9. ACIBADEM CITY CLINIC PHARMACIES EOOD, at address: Sofia, p.b. 1407, 127 Okolovrasten Pat str. (By-pass road);
10. ACIBADEM CITY CLINIC – VARNA MEDICAL CENTER EOOD, at address: Varna, p.b. 9002, 1 Bregalnitsa str.;
11. HEALTHCARE CONSULTING EOOD, at address: Sofia, p.b. 1407, 127 Okolovrasten Pat str. (By-pass road).