Privacy Policy

In this present privacy policy (hereinafter referred to as the "**Policy**") BioSec Group Kft. (registered office: 1119 Budapest, Boglárka utca 32, company registration number: 01-09-994352, hereinafter referred to as the „**Data Controller**") describes how he collects, uses, transfers, transmits and stores his customers' personal information. The Data Controller hereby declares that this present Policy complies with applicable data protection rules and regulations.

The Data Controller may at any time unilaterally change this Policy to comply with the applicable legal provisions, including any changes to the Data Controller's services. Changes to this Policy will be communicated to those affected at the time of the change at www.biosecgroup.com .

If you have any questions about this Policy, please email us at info@biosecgroup.com and our staff is going to answer them. This present Policy and any amendments thereto may be found at www.biosecgroup.com .

At the time of establishing this present Policy the Data Controller was mindful of the following statutes:

- Regulation (EU) No 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Regulation 95/46/EC (hereinafter referred to as the „**GDPR**"),
- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter referred to as the „**Infotv.**")
- Act V of 2013 on the Civil Code (hereinafter referred to as the „**Ptk.**")
- Act C of 2000 on Accounting (hereinafter referred to as the „**Számv. tv.**")
- Act CL of 2017 on the Rules of Taxation (hereinafter referred to as the „**Art.**")
- Act CLV of 1997 on Consumer Protection (hereinafter referred to as the „**Fgy. tv.**")

1. DEFINITIONS

The following terms used in this present Policy shall have the following meaning:
„**data processor**": a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
„**processing of personal data**": 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 data processing**": the marking of stored personal data with the aim of limiting their processing in the future;

„**data controller**": 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; in case the purposes and means of data processing are determined by Union or member state law, the specific aspects of appointing the data controller may also be stipulated by Union or member state law;
„**personal data breach**": 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.
„**pseudonymisation**": 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;
„**biometric data**": 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. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.
„**recipient**": 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;
„**cookie**": A cookie is a short text file sent by our web server to the affected device of the data subject (from any computer, mobile phone or tablet) and which is subsequently read back. There are temporary (or also called "session") cookies that are automatically deleted from the affected device when the browser is closed, and also there are longer lasting cookies that remain on the affected device for a longer period of time (this also depends on the settings of the affected device);
„**data subject**": a person identified or identifiable, directly or indirectly, on the basis of personal data, who must always be a specific person. Only natural persons shall be considered as data subjects, i.e. not legal persons, thus data protection only protects the data of natural persons. On the other hand, personal information includes, for example, the details of an entrepreneur, or a representative of a company (e.g. telephone number, email address, place and time of birth, etc.).
„**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;
„**third party**": 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;
„**third country**": a country that is not a member of the European Union and the European Economic Area. Member States of the European Union may enter into international agreements covering the transfer of personal data to third countries or international organizations, provided that such agreements do not affect other provisions of GDPR or Union law;
„**binding corporate rules**": personal data protection policies which are adhered to by a data controller or data processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

„**profiling**": 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;
„**personal data**": 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. The natural persons may also be associated with online identifiers provided by the devices, applications, devices, and protocols they use, such as IP addresses and cookie identifiers, and other identifiers such as radio frequency identification tags. This can create clues that, in combination with unique identifiers and other information received by the servers, can be used to create a profile of a natural person and to identify that person;
„**filing system**": any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
„**enterprise**": a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
„**data protection officer**": A Data Controller, taking account, in particular, the fact that the operations of its web store Operations include data processing operations which, according to their nature, their scope and / or their purposes, require regular, systematic and extensive monitoring of the data subjects (including without limitation the database of retargeting-based customer consent for behavioural advertising or profiling activities related to the Web Store), hereby appoints a data protection officer.
The data controller shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. The Data Protection Officer shall not accept instructions from any person during the performance of his or her duties, nor may he or she be dismissed, dismissed or penalized in connection with the performance of his or her duties. The Data Protection Officer is directly responsible to the Directorate of the Data Controller, i.e. he / she is entitled and obliged to report directly to the Employer's Directorate on his / her opinion and advice.

Data subjects may contact the Data Protection Officer concerning any and all issues regarding the management of their personal data and the exercise of their rights under the GDPR. The Data Protection Officer shall be bound by the obligation of confidentiality and by the obligation of confidentiality during the performance of his or her duties.

The Data Protection Officer shall essentially perform the following tasks:

a. to inform and give professional advice to the Data Controller and Data Processing Officers on their obligations under the GDPR and other EU or Member State data protection provisions;
b. to verify compliance with the GDPR and other EU or Member State data protection provisions, as well as the Data Controller's internal rules on the protection of personal data, including the assignment of responsibilities, awareness raising and training of personnel involved in data processing operations, and the related audits;
c. to provide technical advice on a privacy impact assessment upon request and monitor the conduct of such an impact assessment pursuant to Article 35 of the GDPR;
d. to cooperate with the supervisory authority; and
e. to serve as a point of contact with the supervisory authority in matters relating to data processing, including the prior consultation referred to in Article 36 of the GDPR and, where appropriate, to consult with it.

The Data Protection Officer shall perform his / her duties with due regard to the risks involved in the processing operations, taking into account the nature, scope, circumstances and purpose of such processing.

The name and contact details of the Data Protection Officer of the Data Controller are set forth in Point 3.1 (b) of this present Policy.

2. DESCRIPTION OF THE PRINCIPLES ON DATA PROCESSING

The Data Controller shall manage personal data lawfully and fairly, in a manner that is transparent to the data subject for clear and lawful purposes as set out in accordance with this present Policy and the documents annexed thereto ("**the purpose limitation principle**"). Data processing shall be limited to what is necessary to achieve the purposes of the Data Controller ("**data minimisation**"). In accordance with the principle of accuracy, the Data Controller shall ensure that the personal data it processes are up-to-date, and to this end, the Data Controller shall take any and all reasonable steps to forthwith delete or rectify any personal data that is inaccurate for the purposes of the data processing ("**principle of accuracy**"). The Data Controller acknowledges that personal data may be stored only for the time necessary to achieve its purposes ("**storage limitation principle**"). The Data Controller shall manage the data in such a way as to ensure adequate security of personal data by appropriate technical or organisational measures, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage to the data ("**integrity and confidentiality**"). The principles contained in this Policy describe our personal data processing practices. Our Privacy Policy applies to paper-based data processing and to any device, website, or other online application operated by the Data Controller which links to or otherwise refers to such data processing. However, where this present Policy refers to a separate privacy policy in the case of each of our data processing activities in relation to their related data processing operations, we also provide separate information or policies to the data subjects. These policies and information notices constitute the annexes to this present Policy and at the same time the integral parts thereof, with the addition that unless expressly provided by such a separate policy or information notice constituting an Annex, then the provisions of this present Policy se Terms and Conditions shall prevail.

3. GENERAL INFORMATION ON DATA PROCESSING

The Data Controller processes the personal data of the data subject in order to provide the services used by the data subject. The Data Controller carries out the processing of personal data for the following purposes and in connection with the activities listed below:

a) the services provided via www.biosecgroup.com ,
b) when signing up for newsletters,
c) during complaint handling

3.1. General information related to the data processing procedures mentioned above:

a) **the Data Controller and his availabilities:** BioSec Group Kft. (registered office: 1119 Budapest, Boglárka utca 32, company registration number: 01-09-994352, phone: +36-1-248-2100, e-mail:, info@biosecgroup.com website: www.biosecgroup.com);

b) **the data protection officer and his availabilities:** Péter Györgydeák info@biosecgroup.com, phone: +36-1 248 2100;

c) **the purpose and legal basis for the processing of personal data:** as specified below for certain data processing operations or in the related Annex;

d) **the period for which the personal data will be stored or the criteria for determining that period:** as specified below for certain data processing operations or in the related Annex;

e) **data subjects** have the right to request from the Data Controller access to, rectification, erasure or restriction of processing of their personal data as defined in this Policy, may also object to the processing of such personal data and may also exercise their right of data portability.

4. GENERAL INFORMATION ON SPECIFIC DATA PROCESSING PROCEDURES

4.1. Data processing in connection with the services provided via www.biosecgroup.com

4.1.1. Registration at www.biosecgroup.com, forum, complaint handling. The purpose of data processing is to use the services of www.biosecgroup.com, to fulfil orders, to document purchase and payment, to fulfil accounting obligations, to maintain customer relations, to analyse customer habits, to have better targeted services and complaint handling.

4.1.2. Data processing when subscribing to the newsletters from www.biosecgroup.com Customers can subscribe to newsletters at the same time as registering on the website. The main purpose of data processing is to send the Data Controller marketing- and professional content-related requests. The Data Controller may use the data for marketing researches and surveys. In accordance with the applicable legal requirements, the Data Controller shall keep records of the natural persons who have subscribed to the newsletter service. The Data Controller shall not send newsletters to natural persons who have not registered themselves.

5. INFORMATION ON THE RIGHTS OF DATA SUBJECTS

5.1. Right to information and access to personal data processed:

The data subject shall have the right to receive feedback from the Data Controller as to whether their personal data is being processed and, if so, to have access to the personal data and the following information:

a) the purposes of data processing;
b) the categories of personal data concerned;
c) the categories of recipients to whom the personal data have been or will be communicated, including in particular third-country recipients or international organizations;
d) where applicable, the period for which the personal data is intended to be stored or, if this is not possible, the criteria for determining this period;
e) the data subject's right to request the data controller to rectify, erase or restrict the processing of personal data concerning him or her and to object to the processing of such personal data;
f) the right to lodge a complaint to a supervisory authority;
g) if the data is not collected from the data subject, all available information on the source thereof;
h) the existence of automated decision-making, including profiling, and, at least in these cases, clear information on the logic used, the significance and the likely consequences for the data subject as a result of such processing.

Where personal is transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate guarantees regarding the transfer.

The Data Controller shall provide the data subject with a copy of the personal data subject to the data processing. The Data Controller may charge a reasonable fee based on administrative costs for any additional copies requested by the data subject. If the data subject has submitted the request electronically, the Data Controller shall provide the information in a widely used electronic format, unless otherwise requested by the data subject.

The right to request a copy referred to in the previous paragraph shall not adversely affect the rights and freedoms of others.

The rights set forth above may be exercised via the contact details provided in clause 13.

5.2. Right of rectification:

At the request of the data subject, the Data Controller shall correct the personal data inaccurate to the data subject without undue delay. Having regard to the purpose of the processing, the data subject shall have the right to request that his or her personal data which are incomplete be supplemented, including by means of a supplementary declaration.

5.3. Right to erasure ('right to be forgotten'):

The data subject shall have the right to delete the personal data relating to him or her without undue delay upon his or her request for any of the following reasons:

a) the personal data is no longer required for the purpose for which they were collected or otherwise processed;
b) the data subject has withdrawn his or her consent as the basis for the processing and there is no other legal basis for the processing;
c) the data subject objects to the processing and there is no overriding legitimate reason for the processing or in case the processing is directly related to the acquisition of the data;
d) the personal data has been unlawfully processed;
e) the personal data has to be deleted in order to comply with a legal obligation under Union or national law applicable to the data controller;
f) the personal data have been collected in connection with the provision of information society services.

Deletion of data shall not be initiated if the processing is necessary for:

a) exercising the right to freedom of expression and information;
b) fulfilling an obligation under Union or Member State law applicable to the data controller for the processing of personal data or in the public interest;
c) preventive health or occupational health purposes, to assess the worker's ability to work, to make a medical diagnosis, to provide health or social care or treatment, or to manage health or social systems and services under Union or Member State law or under contract with a health professional, and the processing of such data is carried out by or under the responsibility of a professional who is subject to the obligation of professional secrecy laid down in Union or national law or in the regulations laid down by the competent authorities of the Member State or by another person also being subject to the obligation of confidentiality laid down in the relevant regulations laid down by the competent bodies of the Member States;
d) the public interest in the field of public health, such as protection against serious cross-border threats to health, or for ensuring the high quality and safety of medicines and medical devices under Union or Member State law which is adequate and specific for providing the safeguards concerning the freedoms of the data subject, and in particular concerning professional secrecy;
e) the public interest and under the responsibility of a professional who is subject to the obligation of professional secrecy laid down in Union or member state law, or the regulations laid down by the competent authorities of the relevant Member State, or by another person; who is also subject to the obligation of confidentiality laid down by Union or member state law or the regulations laid down by the competent bodies of the relevant Member State;
f) archiving, in the public interest, for scientific and historical research or statistical purposes, where the right to erasure would be likely to render impossible or seriously jeopardize this processing; or
g) for the filing, enforcement or defence of legal claims.

5.4. The right to restriction of data processing:

At the request of the data subject, the Data Controller shall restrict data processing if any of the following conditions are met:

a) the data subject disputes the accuracy of his / her personal data, in which case the restriction shall relate to the period during which the data subject can verify the accuracy of his / her personal data;
b) the data processing is unlawful and the data subject opposes the erasure of the data and instead requests that their use be restricted;
c) the Data Controller no longer needs personal data for the purposes of data processing, but the data subject requires such data to make, assert or defend a legal claim; or
d) the data subject has objected to the processing of his / her personal data by the Data Controller on the basis of public or legitimate interest; in this case, the restriction shall apply for the period until it is established whether the legitimate grounds of the data controller prevail over those of the data subject.

Where personal data processing is subject to such restriction, with the exception of storage such personal data shall only be processed with the consent of the data subject or for the purpose of submitting, asserting or defending legal claims or for the purposes of protecting the rights of another natural or legal person, or for the important public interest of the Union or a member state.
The Data Controller shall, in advance, inform the data subject based on whose request data processing has been restricted about lifting the restriction of processing such data.

5.5. The right to data portability:

The data subject shall have the right to receive personal data relating to him or her which he or she has made available to the Data Controller in a structured, widely used, machine-readable format, and to transmit such data to another data controller without being hindered by the data controller to whom he or she has made his or her personal data accessible, in case:

a) the processing is based on consent or a contract; and
b) data is processed in an automated way.

While exercising his or her right to portability of data as described above, the data subject shall have the right to request the direct transfer of his or her personal data between data controllers, where technically feasible.
Exercising the right to data portability shall not prejudice the right to erasure ('right to be forgotten'). The aforementioned right shall not apply where the processing is necessary for the performance processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.
The right to data portability shall not adversely affect the rights and freedoms of others.

5.6. The right to object:

The data subject shall have the right to object at any time to the processing of his or her personal data by the Data Controller for reasons related to his or her situation, if such processing is based on a public interest or while exercising of official authority vested in the Data Controller, or the need to assert the legitimate interests of the Data Controller or a third party, also including profiling based on the aforementioned provisions. In this case, the Data Controller shall not further process the personal data unless he proves that the processing is justified by compelling legitimate reasons, which take precedence over the interests, rights and freedoms of the data subject or that are related to the filing, enforcement or protection of legal claims.

Where personal data is processed for the purpose of direct marketing, the data subject shall have the right to object at any time to the processing of his or her personal data for this purpose, including profiling, in so far as it relates to direct marketing. If the data subject objects to the processing of personal data for the purpose of direct marketing, then his or her personal data shall no longer be processed for this purpose.

Where personal data are processed for scientific and historical research or statistical purposes, the data subject shall have the right to object to the processing of his or her personal data for reasons relating to his or her situation, unless such data processing is necessary for the performance of a task carried out in the public interest.

5.7. The right of withdrawal:

The data subject shall have the right to withdraw his or her consent at any time if the data controller's data processing is based on the data subject's consent. Withdrawal of the consent shall not affect the legality of the consent based data processing prior to such withdrawal.

5.8. Data security measures:

The Data Controller and the server network operator shall protect the data, in addition to reasonably accessible state-of-the-art hardware and software support, in particular against unauthorized access, alteration, transfer, disclosure, deletion or destruction, and against accidental destruction or damage, thus ensuring data security. Data managed by the Data Controller shall, as a rule, be known only to the Data Controller's employees and other contributors involved in the fulfilment of the data processing purposes defined in this Policy, who, by virtue of their employment contract, employment relationship, other legal provisions and the instructions of the Data Controller shall be bound by the obligation of confidentiality with regard to the data which they have access to.

The IT-systems and other data retention places of the Data Controller can be found at the servers of **BioSec Group Kft. (1119 Budapest, Boglárka utca 32)**. In addition, Data Controller uses ERP and www.biosecgroup.com, together with the business operations of Damit Kft.

All data management activities of the Data Controller concerning any and all data processing activities shall be accurately documented. The Data Controller shall keep a data transfer register for the purpose of checking the legality of the data transfer and informing the data subject, which shall include the date of transfer of the processed data, the legal basis, the recipient, the scope of the data and other data specified by the relevant laws stipulating data processing.

5.9. Security of digitally stored personal data

In order to ensure the security of personal data stored on a computer or network, the Data Controller and its data processors, shall act in accordance with the Data Security Policy of Damit Kft., the Data Controller, in particular:

- all access to data is tracked logically,
- maintains virus protection on the personal data management network,
- prevents unauthorized persons from accessing the network using the available IT tools

5.10. Procedure in the case of a request by a data subject to exercise the above rights:

The Data Controller shall, without undue delay, and in any event within one month (30 days) of receipt of the request, inform the data subject of the action taken in response to the interested party's request to exercise the rights set forth in this Policy. Where necessary, taking into account the complexity of the application and the number of applications, this time limit may be extended by a further two months.
The Data Controller shall inform the data subject about the extension of the deadline, indicating the reasons for the delay, within one month from the receipt of the related request. Where necessary, taking into account the complexity of the application and the number of applications, this time limit may be extended by a further two months (60 days). If the data subject has made an application by electronic means, the information shall, as far as possible, be provided by electronic means, unless otherwise requested by the data subject.
If the Data Controller does not act on the data subject's request, he shall inform the data subject without delay, but no later than one month after receipt of the request, of the reasons for the non-action and of the data subject's recourse to a supervisory authority.
The Data Controller shall provide the requested information and information free of charge, insofar as the Data Controller may charge a reasonable amount for the administrative costs of providing the requested information or information or taking the action requested, which are manifestly unfounded or excessive, in particular because of its repetitive nature, or refuse to act on the request.
Unless it proves impossible or requires a disproportionate effort, the Data Controller shall inform any recipient of any rectification, erasure or restriction on the processing of personal data with whom or to whom the personal data have been communicated. At the request of the data subject, the Data Controller shall inform the former about those recipients.

6. DATA PROCESSORS

The Data Controller shall use the Data Processor named in this Policy for the performance of his activities. The Data Processor shall not make any independent decision, but is only entitled to act in accordance with the contract concluded with the Data Controller and the instructions received. The Data Controller controls the work of the Data Processor. The Data Processor is entitled to use further data processors only with the preliminary written consent of the Data Controller.

Data Processor	What personal information can it access? How can it use that personal data (what activities does it carry out for the Data Controller)?	How long can it store the data?
Damit Kft.	Operating a web platform	Service contract of indefinite duration - until the termination of the contract.

7. MEANS TO REPORT OBSERVATIONS, QUESTIONS, COMPLAINTS

If you have any questions or requests regarding your personal information stored in the system and the processing of such information, please send them to info@biosecgroup.com. Please note that we are only able to provide information and take action on the processing of your personal information in your interest if you have credibly verified your identity.
Please be advised that in all matters related to the management of your personal data and the exercise of your rights under the GDPR, data subjects may contact the Data Protection Officer of the Data Controller at the contact details set forth in this present Policy.

8. LEGAL REMEDIES

The Data Controller can be contacted with any questions or comments relating to data processing at any of the contact details provided in this present Policy,
You can also seek redress through the National Authority for Data Protection and Freedom of Information:
Name: National Authority for Data Protection and Freedom of Information
Registered office: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.
Postal address: 1530 Budapest, Pf.: 5.
Telephone: +36-1-391-1400
Fax: +36-1-391-1410
Website: www.naih.hu
E-mail: ugyfelszolgalat@naih.hu
In the event of a violation of his / her rights, the data subject is entitled to initiate legal proceedings against the Data Controller as data controller. The court shall hear the case without delay. The Data Controller shall prove that the data processing complies with the provisions of the applicable legislation. The court hearing the action shall have jurisdiction over the case. At the discretion of the data subject, the lawsuit may also be initiated before the court in the place where the data subject is domiciled or habitually resident.
The Data Controller shall indemnify for damage caused to others due to unlawful processing of the data of the data subject or violation of data security requirements. In the event of a violation of his or her privacy, the data subject is entitled to claim damages (Section 2:52 of the Civil Code). The Data Controller is not liable if the damage was caused by an unavoidable cause outside the scope of the data processing. The Data Controller shall not reimburse the damage or shall not be expected to pay compensation for aggravated damages in so far as the occurrence of the damage is due to the intentional or grossly negligent conduct of the injured party.

Last revised on: 11.18.2019.