1. Introduction

For the performance of its activities **Sabiex SA** (hereinafter referred to as "the Company") processes various data, both commercial and personal data. This policy concerns the processing of personal data by the Company. The personal data of different categories of identifiable persons such as employees, customers and suppliers and possible other stakeholders are processed.

The Company understands the importance of the protection of personal data and the concerns of its employees, (contact persons of) customers, (contact persons of) suppliers and other persons with whom it has contact regarding the processing of their personal data. The Company always carefully considers the protection of personal data during the different personal data processing operations.

Different persons within the organisation may have access to the personal data of its employees (the term employees shall include: managers and everyone who works for the Company, including independent service providers and consultants, temporary workers such as interim workers, interns, student workers, volunteers, ex-employees) and other individuals (customers and suppliers) during the performance of their duties. Each of these persons within the Company is bound by this policy on the protection of personal data.

The applicable data protection legislation imposes obligations on the Company regarding the way in which it must process data. In addition, the legislation provides for rights for the persons whose data are processed, so that they have more control over their own personal data.

This policy gives an overview of the general obligations under the data protection legislation which the Company and its employees must comply with. Compliance with this policy is important for the following reasons:

- Compliance with data protection legislation is a legal obligation and failure comply with these duties can lead to liability, sanctions and fines;
- Compliance with data protection legislation leads to more satisfactory and efficient processing of personal data;
- Compliance with data protection legislation is the basis for a relationship of trust between the Company and its business relations, consumers and its employees.

2. Scope

This policy is applicable to the Company which processes personal data and contains the guidelines which each personal data processing operation must comply with. This processing occurs either fully or partly via automated processes which are part of a structured filing system or will become part of a structured filing system.

3. Contact person for the protection of personal data

The Company has appointed a responsible person, supported by a team, to ensure the implementation and compliance with data protection legislation and this policy.

The person responsible for data protection can be contacted by e-mail to privacy@sabiex.be. In order to exercise your rights, please refer to Article 8 of this policy.

4. Definitions

The applicable data protection legislation uses specific language and refers to an abstract matter. Hereafter you will find several definitions in order to enable you to better understand the terminology, and by extension, this policy.

4.1. Data protection legislation

Various legislation can apply, depending on the concrete application in which personal data are processed.

The basic principles and obligations are indicated in Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

This regulation is also known as the General Data Protection Regulation (GDPR).

4.2. Personal data

Personal data concern all information about an identified or identifiable natural person, also known as the data subject. A person is considered as identifiable when a natural person can be directly or indirectly identified, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more elements that are characteristic of the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.

4.3. Controller

The controller is a natural person or legal person (for example a company), a public authority, agency or other body which, alone or jointly with others, determines the purposes and means for the processing of personal data.

For example,the Company is a legal person which is the controller that processes the personal data of its employees in the context of its personnel management.

4.4. Processor

The processor is a natural person or legal person, a public authority, agency or other body that processes personal data on behalf of and only on instructions from the controller.

4.5. Processing personal data

Processing personal data means any operation or set of operations which is performed upon personal data or a set of personal data, whether or not by automatic means (e.g. software), such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

An example of processing personal data is when the organisation collects and saves the contact details of its clients' contact persons in the organisation's Client Relationship Management software system or in a paper filing system.

4.6. Filing system

A filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

This implies both electronic structured filing systems by means of the use of software or cloud applications, and paper files and filing systems, provided that these filing systems are organised and structured in a logical way by connecting them to individuals or which are connected to individuals on the basis of criteria.

5. Principles applicable when collecting and processing personal data

As well as the use of specific language, data protection legislation has several basic principles which every controller must comply with in order to be in accordance with this legislation. In the event of doubt regarding the application of these principles in a concrete case, you can always contact the responsible for data protection for further explanations, and according to the procedure described in Article 8.

Data protection legislation provides that personal data must be processed in agreement with the various basic principles and the conditions that result from them.

5.1. Lawfulness

Data protection legislation provides that personal data must be processed fairly and lawfully with respect to the data subject.

In order to process personal data lawfully, a legal basis must exist. In principle, personal data can only be processed when:

- The data subject has given his or her consent. The organisation shall inform the person concerned at the latest before the data is collected about the purpose for which consent is required, which personal data will be collected for the processing, the right to revoke consent, the possible consequences for the data subject in the context of automated individual decision-making and profiling, and transfer to third countries.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation which is imposed upon the organisation;
- Processing is necessary in order to protect the vital interests of the data subject or another natural person;
- 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 organisation, which acts as the controller;
- Processing is necessary for the purposes of the legitimate interests pursued by the organisation as a controller or the interests of a third party, except where the fundamental rights and freedoms of the data subject regarding the protection of his or her personal data override these interests.

If you have given your consent for a specific processing purpose to the organisation in order to process your data for that purpose, you can withdraw this consent at any time. The organisation will then stop any further processing of your data for which you gave consent and will inform you of the possible consequences of your withdrawal of consent. If the organisation processes your personal data for other purposes and in order to do so it refers to other legal bases, it will still be able to process your personal data.

The organisation ensures that it always refers to at least one of the above-mentioned legal bases when it processes personal data. If you have questions about the applicable legal basis that the organisation is referring to, you can always contact the person in charge of data protection in accordance with the procedure provided in Article 8.

Some categories of personal data are of a sensitive nature and data protection legislation also has a stricter regime for these special categories of personal data (also known as ‘sensitive personal data’). These are data concerning race or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and processing of genetic data, biometric data for the unique identification of a person, or data about health, sexual behaviour or sexual orientation. Data relating to criminal offences or convictions also form a special category.

In principle it is forbidden to process these sensitive personal data, unless the organisation can refer to one of the exceptions. In a specific limited number of cases, the organisation must process sensitive personal data. In these cases, the data subject will be informed in

advance. For these specific purposes, the organisation will provide the person concerned with detailed information in advance about the specific purposes and the legal basis of the processing. For more information about the processing of sensitive personal data by the organisation, you can always contact the person in charge of data protection according to the procedure described in Article 8 of this policy.

5.2. Fairness

The organisation ensures that personal data shall be processed:

- For specific, explicit and legitimate purposes and may not be processed further in a way incompatible with the initial purposes for which the data were collected. The organisation shall always clearly communicate the purposes before starting the processing.
- This processing shall be limited to what is necessary for the purposes for which the data were collected. If possible, the organisation will anonymise the data or use pseudonyms in order to limit the impact for the data subject as much as possible. This means that the name or identifier will be replaced so that it is difficult or even impossible to identify an individual.
- Limited in time and only as necessary for the specific purpose.
- Accurately, and the data shall be updated where necessary. The organisation shall take all reasonable measures to erase or update the personal data, taking into account the purposes for which they are processed.

5.3. Transparency

The organisation processes personal data which, in principle, it has received directly from the data subject. The organisation which processes the data subject's personal data shall always inform data subjects about the following matters:

- identity and contact details of the controller
- the contact details of the responsible for data protection
- processing purposes and legal basis
- if the personal data processing is supported by a legitimate interest, an explanation of this interest
- categories of receivers of the personal data
- transfer of personal data to third countries (outside the EU) or international organisations (+ on what basis)
- Time limit for the storage of personal data or the criteria used to determine the time limit
- Data subject's rights (including the right to revoke consent)
- The right to lodge a complaint with the supervisory authority
- Explanation when the transmission of personal data is a contractual or legal obligation
- The logic behind automated decision-making processes and the possible legal consequences for the data subject

- If the organisation receives personal data from a third party, it shall clearly inform the data subject about the categories of personal data which it received from this third party and will also make this third party known to the data subject.

When the data subject already has all the information, the organisation will not inform the data subject unnecessarily about the processing of his or her personal data.
If the organisation processes personal data for other purposes which are incompatible with the initial purposes for which the data were initially collected (the new purpose does not appear to be described in the initial information note and the data subject cannot assume that his/her personal data will also be processed for this new purpose), the organisation shall take all the necessary measures to process these personal data lawfully, and shall inform the data subject about this.

The organisation can disclose the information both on a collective and individual basis and shall continue to ensure that it is drafted in plain, intelligible language.

Specific legislation may contain exceptions or set additional requirements which the organisation must comply with, with respect to the provision of information to data subjects. These mandatory legal provisions take precedence over this policy.

5.4. Confidentitality and integrity

The company takes the required technical and organisational measures to ensure that the processing of personal data always takes place with the appropriate guarantees, so that the data are protected against accidental loss and against unlawful processing, destruction or damage. The organisation has, when choosing the proper security measures, considered the nature, context, purpose and scope of the processing, the possible risks when processing the personal data, the costs for the implementation of the measures and the state of the art.

These measures are applicable to the physical access to personal data, access to the personal data via computers, servers, networks or other IT hardware and software applications and databases. In addition to the technical and organisational measures, the organisation's employees who have access to personal data during the performance of their duties, are bound by different obligations in order to guarantee the confidentiality and integrity of personal data, as summarised in Article 9 of this policy.

The organisation will organise training courses for the employees who will process personal data on the instructions of the organisation when carrying out their duties. The employees may only process the personal data at the organisation's instruction or if the law requires them to do so. The organisation shall also implement access rights, so that the employees only have access to the data they need when performing their duties. The employees who have access to personal data shall sign a confidentiality agreement.

The organisation shall ensure that the third parties that receive personal data from the organisation will comply with the applicable data protection legislation and this policy.

6. Transfer of personal data

In some cases, the organisation may be obliged to transfer your personal data to third party receivers. In any event, these personal data are only transferred on a need-to-know basis to these receivers who carry out the processing for specific purposes. The organisation shall always observe the necessary security measures when transferring the data and with respect to the receivers, in order to guarantee the confidentiality and integrity of the personal data.
The transfer to third parties can take several forms, as described below.

6.1. Transfer to processors

The organisation can ask a third party, a processor, to process personal data, on behalf of and only on instructions from the organisation. The processor may not process these personal data for its own purposes which are independent of the purposes for which the organisation uses the processor.

The organisation can opt to work with these processors which deliver services at the organisation's request, for travel agencies, rental services, medical and other professional consultancy services, etc.

The organisation shall only use processors and provide them with personal data when processor agreements which meet the legal requirements are concluded with the processors. The GDPR provides, among other things, that the agreement must contain a clause which indicates that the processor may only process the personal data at the organisation's instruction; that the processor must provide the organisation with assistance when it requests it; that personal data must remain confidential, etc.

Part of this processor agreement also concerns the security measures which the processor must implement before processing the personal data and must have throughout the entire duration of the processing in order to ensure the confidentiality and integrity of the data.

The organisation shall take the necessary measures if it establishes that its processors do not comply with the obligations in the agreement.

A standard processor agreement is available from the responsible for data protection.

6.2. Transfer to third countries – outside the European Economic Area

It is also possible for the organisation to transfer your personal data to parties that are based in third countries, these are countries outside the European Economic Area (i.e. The European Union, Norway, Iceland and Liechtenstein).

Such a transfer is possible if the country where the receiver is based offers sufficient legal guarantees to protect your personal data and which the European Commission has

assessed as being adequate. In other cases, the organisation has concluded a standard contract with the receiver so that equivalent or similar protection to that offered in Europe is offered.

For cases in which this did not or cannot happen, the organisation can always pass on the data subject's personal data if it obtains consent from the data subject, within the limits of the relationship which the data subject has with the organisation. In order to ensure transfer and thus processing is possible in these cases too, where appropriate, the organisation shall thus ask the data subject whether he/she agrees to this occasional transfer to third countries.

If more information or a copy of the guarantees for these international transfers are desired, the procedure as described under Article 8 can always be followed.

7. Time limit for the storage of personal data

The organisation shall not store personal data any longer than necessary for the specific purpose for which the data were collected. After the final time limit has passed, the organisation shall delete or anonymise the personal data. The organisation shall anonymise the data if it still wishes to use them for statistics. The organisation may store the personal data for a longer period for its dispute management, research or archiving purposes.

8. Rights of individual data subjects

Data protection legislation provides for different rights for data subjects with respect to the processing of personal data so that the data subject can still exercise sufficient control over the processing of his or her personal data.

The organisation tries, via current policy, to already provide as much information as possible to the data subjects in order to be as transparent as possible with respect to the processing of personal data. This general policy must be read together with more specific information notes which give more explanations about the organisation's specific processing purposes.

The organisation understands that the data subject may still have questions or desire additional clarifications with respect to the processing of his or her personal data. The organisation thus understands the importance of the rights and shall therefore comply with these rights, considering the legal limitations in the exercising of these rights. The different rights are described in detail below.

8.1. Right of access/inspection

The data subject has the right to obtain confirmation from the organisation of whether or not his or her personal data are being processed. If his or her data are being processed, the data subject may request the right to consult his or her personal data.

The organisation shall inform the data subject about the following matters:

- the processing purposes;
- the categories of personal data concerned;
- the receivers or categories of receivers to which the personal data are supplied;
- transfer to receivers in third countries or international organisations;
- if possible, the period during which it is expected that the personal data will be saved, or if this is not possible, the criteria used to determine this period;
- that the data subject has the right to ask the organisation to correct or erase personal data, or to limit the processing of his or her personal data, as well as the right to object to this processing;
- that the data subject has the right to lodge a complaint with a supervisory authority;
- if the personal data are not collected from the data subject, all available information about the source of the data;
- the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The organisation shall also supply a copy of the personal data that are being processed. For any further copies requested by the data subject, the controller may charge a reasonable fee.

8.2. Right to rectification

When the data subject establishes that the organisation has incorrect or incomplete data about him/her, the data subject always has the right to inform the organisation of this fact so that appropriate action can be taken to rectify or supplement these data. It is the data subject's responsibility to provide correct personal data to the organisation.

8.3. Right to be forgotten

The data subject can ask to have his or her personal data erased if the processing is not in accordance with data protection legislation and within the limits of the law (Article 17 GDPR).

8.4. Right to restriction of processing

The data subject may ask to have the processing restricted if:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to check their accuracy;
- the processing is unlawful and the data subject opposes the erasure of the data;
- the organisation no longer needs the data, but the data subject requests that they not be removed, given that he or she needs them for the exercise or defence of legal claims;
- he or she has objected to processing, pending the verification whether the legitimate grounds of the controller override those of the data subject.

8.5. Right to data portability

The data subject has the right to obtain his or her personal data which he or she provided to the organisation in a structured, commonly-used and machine-readable format. The data subject has the right to have those personal data transmitted to another controller (directly by the organisation). This is possible if the data subject has consented to the processing and if the processing is carried out via an automated process.

8.6. Right to object

When personal data are processed for direct marketing purposes (including profiling), the data subject can always object to this processing.

The data subject can also object to processing due to a specific situation regarding the data subject. The organisation shall stop processing the personal data unless the organisation demonstrates compelling legitimate grounds for the processing which override the interests of the data subject or for the exercise or defence of legal claims.

8.7. The right to withdraw consent

If you have given your consent for a specific processing purpose to the organisation in order to process your data, you can withdraw this consent at any time by sending an e-mail.

8.8. Procedure for exercising rights and other provisions

The data subject may exercise his or her rights by sending an e-mail to the responsible for data protection via email to privacy@sabiex.be. The organisation can ask the data subject to identify himself /herself in order to ensure that it is indeed the data subject requesting to exercise his or her rights.

If you have any questions about the application of the principles or the organisation's (legal) obligations, you can always contact the responsible for data protection via email to privacy@sabiex.be.

In principle the organisation shall respond to the data subject's request within one month. If not, the organisation shall inform the data subject why the request received no response or why it did not receive a response in good time. The organisation shall take the necessary measures to inform the receivers of the data subject's personal data about exercising the right to correction, right to erasure or the limitation of processing by the data subject.

9. Employees' responsibilities

The organisation expects its employees to comply with this policy and it ensures that the persons it is responsible for comply with this policy.

It is crucially important that the employees understand the aims of this policy and familiarise themselves with it so that they can comply with the provisions contained in this policy. The employees must therefore:

- Process the personal data of fellow employees, clients, etc. in a regular and proper way in accordance with the applicable legislation, the employer's instructions and the company's privacy policy, and where personal data are processed confidentially and considering their integrity;
- Ask advice from their manager, the person responsible for data protection if they have doubts about the application of this policy or compliance with data protection legislation when performing their duties;
- Only process personal data when this is required for the performance of duties / on instructions from the organisation;
- Follow training courses about the confidential processing of personal data and the general principles and obligations which result from data protection legislation;
- Provide assistance to the person responsible for data protection;
- Not save any copies of personal data on their desktop or personal portable storage if the organisation has centralised and secure storage, given that saving your own files or copies can lead to incorrect personal data and higher risks of breaches.
- Immediately inform the person responsible for data protection if he or she establishes a potential or actual breach of personal data or personal data legislation.

10. Compliance

Each person who has access to personal data processed by the organisation must comply with this policy. Non-compliance with this policy can lead to disciplinary measures/sanctions such as a warning, dismissal or any other sanction permitted by law, without prejudice to the right to initiate civil or criminal proceedings.

11. Audit and review

The organisation reserves the right to adjust and review this policy when it deems necessary and to remain coherent with the legal obligations and/or recommendations of the competent supervisory authority for data protection.

.

The organisation shall inform the person responsible for data protection when it is impossible for it to comply with this policy due to mandatory legal provisions which are imposed upon the organisation.

12. Entry into force

This policy applies as of May 25, 2018.

13. Technical and organisational security measures

Organisational measures
- Security Officer
- Security and risk plan
- Security directives
- Raising awareness among staff through training and providing information
- Reporting of physical/technical incidents
- Disciplinary consequences if one of the measures is not complied with
- Recovery plan and emergency plan in the event of physical/ technical incidents
- Plan ensuring that the effectiveness of the organisational/technical measures are regularly checked/evaluated and assessed
- Periodic check of the suitability of the processing systems
Technical measures
- Back-up system
- Measures for fire, a break-in or water damage or physical/technical incidents
- Access control (physical and logical)
- Authentication system
- Password policy
- User ID policy
- Patching
- Antivirus
- Firewall
- Network security
- Surveillance, research and maintenance of the systems
- Encryption