PERSONAL DATA PROTECTION POLICY

Element sp. z o.o. S.K.A. with its registered seat in Gdynia
at al. Zwycięstwa 96/98 lok. C1.04, 81-451 Gdynia

Date of last update: 23 January 2020

TABLE OF CONTENTS

1. Introductory information

A. Definitions

1.1. For the purpose of the Personal Data Protection Policy:

a) „**The Controller**" means **Element spółka z ograniczoną odpowiedzialnością spółka komandytowo-akcyjna** with its registered seat in Gdynia, al. Zwycięstwa 96/98 lok. C1.04, 81-451 Gdynia, entered into the register of entrepreneurs maintained by the Regional Court Gdansk – North in Gdansk, 8th Economic Division of the National Court Register under KRS number 0000810330, Tax Identification Number (NIP) 5862349944, Statistical Number (REGON) 384697791,

b) „**The Controller of the IT Systems**" means a person acting under the authority of the Controller who manages the Information System and supervises it,

c) „**password**" means a string of letters, numbers or other characters, known only to the Controller of the IT Systems and known only to the User,

d) „**user ID**" means a string of letters, numbers or other characters, unequivocally identifying user in the Controller's IT System,

e) „**the supervisory body**" means the President of the Personal Data Protection Office,

f) „**Personal Data Protection Policy**" means this document,

g) „**GDPR**" means the Regulation of the European Parliament and of the Council (EU) 2016/679 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 (General Data Protection Regulation) (EU Journal of Laws L 119, of 04.05.2016, p 1),

h) „**IT System**" means a set of cooperating devices, programs, information processing procedures and software used to process data,

i) „**authentication**" means an action, the purpose of which is to verify the entity's declared identity,

j) „**user**" means a person authorised to work in the Controller's IT System.

1.2. For the purpose of the Personal Data Protection Policy, the definitions specified in the GDPR also apply, provided they do not contradict the definitions contained in section 1.1. above.

B. The aim of creating The Personal Data Protection Policy

1.3. Personal Data Protection Policy is a feature implemented by the Controller in accordance with Article 24 paragraph 1 and 2 of the GDPR, the purpose of which is to introduce the procedure for handling Personal Data in the company run by the Controller, the processing of personal data pursuant to this procedure will be done in accordance with the GDPR and this procedure shall make it possible to demonstrate compliance with the GDPR.

1.4. Personal Data Protection Policy lays down in particular, what other technical and organisational measures have been implemented with this purpose by the Controller, taking into account the nature, scope, context and purposes of processing as well as the risk of violation of the rights or freedoms of natural persons with different probability and scale of the threat.

C. Scope of application of Personal Data Protection Policy

1.5. Personal Data Protection Policy applies to processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

1.6. Every person in the Controller undertaking's organisational structure is required to apply Personal Data Protection Policy, independently of the character of the contractual relationship between the Controller and this person. In particular, this applies to members of the Controller, his/her employees, persons employed under civil contracts, trainees.

2. Rules for the processing of personal data

A. Basic rules for the processing of personal data

2.1. The Controller will ensure that personal data are processed as required by GDPR, other generally applicable provisions of law and best practices. Therefore, personal data should absolutely be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject,

b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes,

c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed,

d) accurate and if necessary kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay,

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed,

f) processed in a manner providing their safety, including protection from unauthorised or unlawful processing and accidental loss, destruction or injury, by appropriate technical and organisational measures.

2.2. The Controller shall not carry out processing that are likely to present high risks to the rights and freedoms of natural persons. The commencement of such processing shall require the Controller's prior assessment of the effects of planned processing operations for the protection of personal data in accordance with art. 35 of the GDPR.

B. Basis of personal data processing

2.3. The processing of personal data by the Controller shall only take place if—to the extent when at least one of the following conditions is fulfilled:

a) the data subject gave the assent to process the data in one or more specific purposes,

b) 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,

c) processing is necessary for compliance with a legal obligation to which the controller is subject,

d) the processing of the data is necessary to protect vital interests of the data subject or other natural person,

e) 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 Controller,

f) processing is necessary for the purposes of the legitimate interests pursued by the Controller or third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

2.4. The basis of the processing referred to in points c) and e) of paragraph 2.3 above, must be provided for in Union law or Polish law. The purpose of processing must be stated in that legal basis or, in the case of processing referred to in point e) of paragraph 2.3 above – 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 Controller.

C. Application of the "privacy by design" principle

2.5. The Controller ensures the use of procedures for implementing changes, projects or investments that at the earliest possible stage (privacy-by-design) ensure the assessment of the impact of the implemented solution on the protection of personal data.

2.6. The Controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, which are designed to implement data-protection principles and to provide the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

2.7. The Controller shall implement appropriate technical and organisational measures taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

D. Application of the "privacy by default" principle

2.8. The Controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

E. The recording of data processing operations

2.9. The Controller keeps an electronic register of data processing operations in accordance with art. 30 section 1 of the GDPR.

2.10. Register of processing operations on personal data is a tool enabling the Controller to implement the principle of accountability and is subject to disclosure at request of the supervisory body.

F. The entrustment of personal data processing

2.11. The Controller may entrust the processing of personal data to processor only on the principles consistent with the requirements of art. 28 of the GDPR.

2.12. Before entrusting the processing of personal data, the Controller, to the extent possible, obtains information about the processor’s current practices in the field of personal data protection.

3. Security of Personal Data

A. Access to personal data processed by the Controller

3.1. Only persons holding of an authorization issued by the Controller to process personal data in accordance with the template constituting appendix A to the Personal Data Protection Policy are allowed to process personal data.

3.2. In the authorization to process personal data, the Controller precisely indicates temporal and substantive scope of the authorization. The authorization shall be drawn up so that makes its scope clear - it must not arouse any interpretation doubts. In particular:

a) the scope of authorization should clearly refer to the processing operations of personal data listed and described in the register of data processing operations referred to in item 2.9 above,

b) the scope of authorization should include an explanation of whether the authorization covers the processing of personal data in the IT system, outside it, or both.

3.3. Any person acting under the authority of the Controller and having access to personal data shall process them only on the Controller's instructions, unless required by Union or Member State law.

3.4. Before undertaking the processing of personal data, each person acting under the authority of the Controller will be made aware of the Personal Data Protection Policy and undertake to comply with it according to the template constituting appendix B to the Personal Data Protection Policy.

3.5. The Controller of the IT Systems shall keep the register of persons authorised to carry out the processing of personal data in accordance with the template constituting appendix C to the Personal Data Protection Policy. The entry in the register may only be based on a document drawn up by the Controller.

B. The Controller of the IT Systems

3.6. The Controller shall appoint a controller of the IT systems in accordance with the template constituting appendix D to the Personal Data Protection Policy.

3.7. The Controller shall ensure that each person obliged to apply the Personal Data Protection Policy has knowledge of who is the Controller of the IT Systems.

3.8. The Controller's of the IT Systems tasks include the management of the Controller's Information System and supervision of that System, including:

a) preventing access to the IT System by unauthorized persons,

b) assigning user IDs and passwords to the IT system,

c) ensuring compliance of the rights of IT System users with the register of persons authorized to process personal data,

d) supervising the operation of user authentication mechanisms and controlling access to personal data,

e) exercising supervision over repair works, maintenance and decommissioning of computer devices on which personal data are stored, over making backups, storaging and periodic checking for their further suitability for data recovery in the event of IT System failure,

f) taking action to ensure the reliability of power supply for computers and other devices affecting security of data processing and to ensure secure data exchange in the internal network and secure data transmission via the telecommunications network,

g) ensuring the application of technical and organizational measures provided for in the Personal Data Protection Policy and assessing their suitability for ensuring the security of personal data processing in the IT System.

3.9. Moreover, the Controller of the IT Systems shall be obliged to perform other obligations set out in the Personal Data Protection Policy and Controller's instructions.

C. The main security principles applicable to the processing of personal data

3.10. Any person who has access to personal data is responsible for their security, including in particular, processing them in a manner consistent with the Personal Data Protection Policy.

3.11. Persons having access to personal data may not disclose or use them either at the workplace or outside of it, in a way that goes beyond activities related to their processing within the scope of official duties under the authorization to process personal data granted by the Controller. This prohibition also applies after the termination of the legal relationship connecting a person having access to personal data with the Controller.

3.12. It is unacceptable to take materials containing personal data outside the designated place of their processing without the Controller's explicit prior instruction.

D. Technical and organizational measures to ensure the security of personal data

3.13. Personal Data shall be processed in locations indicated for this purpose. These locations are protected by lockable doors and anti-theft alarm system, and the windows in these locations are protected by gratings, blinds or anti-burglar film. These locations are also protected against the effects of fire by means of a fire protection system and / or a free-standing fire extinguisher.

3.14. The presence of bystanders in the location where personal data are processed is only allowed in the presence of a person authorized to process personal data and provided that the way of securing such data precludes accidental disclosure to a bystander.

3.15. Buildings or rooms where personal data are processed shall be kept locked in the absence of persons authorized by the Controller to process personal data. Persons with keys to these buildings or rooms are required to secure them.

3.16. Access to buildings and rooms where personal data are processed is protected by the security service in the absence of persons authorized to process personal data.

3.17. In the place of processing personal data recorded in paper form, the so-called the "clean desk" principle applies. This principle means not leaving materials containing personal data in a place where they can be physically accessed by unauthorized persons.

3.18. The sets of personal data in paper form are stored in lockers.

3.19. Destruction of all materials containing personal data must be done in a way that makes it impossible to read the content contained in them, e.g. using shredders.

3.20. Personal data processed in the IT System shall be secured by making back-up copies of personal data and data processing programs. Backup copies are stored in a different room than the one in which the server is located, where personal data are processed on an ongoing basis, and deleted immediately after they cease to be usable.

3.21. Computer monitors on which personal data are processed shall be set up in such a way that prevents access to content displayed on them by unauthorized persons.

3.22. Provision shall be made for the training, instructions and explanations of all persons who have access to personal data, necessary to guarantee the safety of the personal data processing.

3.23. In the IT system used to process personal data, data access control mechanisms are used. Each user of the IT system is assigned a user identification (user ID), and access to personal data is only possible after entering that identification and authenticating with a password consisting of at least 8 characters and containing uppercase and lowercase letters and numbers or special characters. The password is changed at least every 30 days.

3.24. User ID (user identification) that has lost the authorization to process personal data can not be assigned to another person.

3.25. IT System used to process personal data is protected, in particular against:

a) operation of software whose purpose is to obtain unauthorized access to the IT system,

b) data loss caused by a power failure or power source disturbance,

c) threats from the public network.

3.26. The only person authorized to install new software and make changes in the software already installed on the Controller's computers is the Controller of the IT Systems.

E. Specific additional measures for the protection of personal data on mobile devices and data carriers

3.27. Person who uses mobile devices or data carriers containing personal data shall be obliged to exercise appropriate care during their transportation, storage and operation, as well as apply password protection and cryptographic protection measures to personal data being processed.

3.28. Mobile devices and data carriers must not be left unsupervised in public places, hotels, cars and other places to which bystanders may gain access.

3.29. Mobile devices and data carriers must be transported in relevant covers, if available.

3.30. Mobile devices and data carriers must be protected against damage, in particular the producer's recommendations regarding equipment protection should be followed.

3.31. The use of mobile devices and data carriers in public places is only allowed if the risk of accidental disclosure of personal data to a bystander is excluded.

3.32. Mobile devices and data carriers may be used only by persons indicated by the Controller.

3.33. Person who uses mobile devices or data carriers shall be obliged to make backup copies of personal data and data processing programs according to the instructions provided to her/him by the Controller or the Controller of the IT Systems.

3.34. Person who uses mobile devices or data carriers shall be obliged to immediately notify the Controller or the Controller of the IT Systems of their loss or damage.

4. The Data Protection Officer

4.1. The Controller has appointed Data Protection Officer within the meaning of the GDPR. Contact details: inspektorodo@elementapp.ai

5. The procedure applicable in the event of a personal data breach

A. Internal proceedings

5.1. In the case of a personal data breach, each person shall without undue delay, after having become aware of it, notify the personal data breach to the Controller of the IT Systems.

5.2. If it possible and justified given the circumstances, the person making the notification shall:

a) immediately take the necessary measures to stop the adverse effects of the infringement,

b) identify the causes and perpetrators of the infringement,

c) refrain from further planned activities that involve the infringement and may hinder its documentation and analysis,

d) document (pre-)existing safety violation,

e) not leave the place of the incident leading to the breach until the Controller of the IT Systems arrives, if he deems this necessary.

5.3. In the case of notification of personal data breach, the Controller of the IT Systems shall immediately take all the necessary steps to clarify the circumstances of a breach and minimize its effects. The Controller of the IT Systems shall notify the Controller without undue delay of any action taken by him, who may issue binding instructions as to how to proceed in the case of a breach.

5.4. Unless it appears that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, the Controller of the IT Systems shall be obliged to immediately prepare a draft notification of a personal data breach to the supervisory body and forward this draft to the Controller. The draft notification shall at least:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) contain the name, surname and contact details of the Controller of the IT Systems as contact point where more information can be obtained;

c) describe the likely consequences of the personal data breach,

d) describe the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

5.5. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller of the IT Systems shall be obliged to immediately prepare a draft notification of a personal data breach to the data

subject and forward this draft to the Controller. The draft notification shall describe in clear and plain language the nature of the personal data breach and shall at least:

a) contain the name, surname and contact details of the Controller of the IT Systems as contact point where more information can be obtained,

b) describe the likely consequences of the personal data breach,

c) describe the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

5.6. The obligation to prepare the draft notification by the Controller of the IT Systems referred to in paragraph 5.5 above shall not be required in the following cases:

a) the Controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

b) the Controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;

c) the communication to the data subject would involve disproportionate effort. In such a case, the Controller of the IT Systems shall be obliged to prepare a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

5.7. The controller, taking into account the information and documents provided by the Controller of the IT Systems, shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory body to verify compliance with art. 33 of the GDPR.

B. External proceedings

5.8. In the case of a personal data breach, the Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory body, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory body is not made within 72 hours, it shall be accompanied by reasons for the delay. The notification shall at least:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned,

b) contain the name, surname and contact details of the Controller of the IT Systems as contact point where more information can be obtained,

c) describe the likely consequences of the personal data breach,

d) describe the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

5.9. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided by the Controller to the supervisory body in phases without undue further delay.

5.10. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall communicate the personal data breach to the data subject without undue delay. The notification shall describe in clear and plain language the nature of the personal data breach and shall at least:

a) contain the name, surname and contact details of the Controller of the IT Systems as contact point where more information can be obtained,

b) describe the likely consequences of the personal data breach,

c) describe the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

5.11. The notification referred to in paragraph 5.10 above shall not be required in the following cases:

a) the Controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption,

b) the Controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize,

c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

6. The update of personal data protection measures

6.1. The Controller shall continuously assess the risk of violation of the rights or freedoms of natural persons in relation to the processing of personal data, taking into account the nature, scope, context and purposes of processing.

6.2. Technical and organizational measures implemented by the Controller to ensure that the processing would take place in accordance with the GDPR and would be able to demonstrate this, in particular the Personal Data Protection Policy, shall be reviewed and updated, if necessary.

6.3. The need to review technical and organizational measures occurs at least when the nature, scope, context or purpose of the processing or the likelihood or level of risk of violation the rights and freedoms of natural persons changes.

6.4. The need to review technical and organizational measures occurs at least when the likelihood or level of risk of violation the rights and freedoms of natural persons changes.

7. Final provisions

7.1. It is the responsibility of members of the Controller to comply with the Personal Data Protection Policy.

7.2. The Appendixes to this Personal Data Protection Policy shall form an integral part thereof.

8. The Appendixes

A. Model of authorisation to process personal data

place, date ..... 20..... r.

AUTHORISATION NO_____TO PROCESS PERSONAL DATA

Acting on behalf of the **Element spółka z ograniczoną odpowiedzialnością spółka komandytowo-akcyjna** with its registered seat in Gdynia, al. Zwycięstwa 96/98 lok. C1.04, 81-451 Gdynia, entered into the register of entrepreneurs maintained by the Regional Court Gdansk – North in Gdansk, 8th Economic Division of the National Court Register under KRS number 0000810330, Tax Identification Number (NIP) 5862349944, Statistical Number (REGON) 384697791, ("**The Controller**"), pursuant to Article 5 section 1 letter f) in conjunction with Article 29 of the Regulation of the European Parliament and of the Council (EU) 2016/679 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 (General Data Protection Regulation) (EU Journal of Laws L 119, of 04.05.2016, p 1),

I hereby authorise

Mr./Ms.:.....

Position/ Function: .....

to process personal data, only on instructions from the Controller, in the following scope:

Temporal scope of the authorization:

until withdrawal / to ……..*

The substantive scope of the authorization:

a) ……..

b) ……..

c) ……..

……..
(signature of the person authorised to issue and revoke the authorisations)

Authorisation received

……..
(date and signature of the authorized person)

*delete as appropriate

B. Model of confirmation of knowledge of the Personal Data Protection Policy

place, date ..... 20..... r.

The confirmation of knowledge of the Personal Data Protection Policy

I, the undersigned, ...,

herein declare that I have acquainted myself with the Personal Data Protection Policy binding in the **Element spółka z ograniczoną odpowiedzialnością spółka komandytowo-akcyjna** with its registered seat in Gdynia, al. Zwycięstwa 96/98 lok. C1.04, 81-451 Gdynia, entered into the register of entrepreneurs maintained by the Regional Court Gdansk – North in Gdansk, 8th Economic Division of the National Court Register under KRS number 0000810330, Tax Identification Number (NIP) 5862349944, Statistical Number (REGON) 384697791,
(„**The Controller**"),

and **I undertake** to comply with it.

In particular, **hereby I acknowledge and accept** that personal data processed by the Controller I shall not disclose or use them either at the workplace or outside of it, in a way that goes beyond activities related to their processing within the scope of official duties under the authorization to process personal data granted to me by the Controller. I undertake to comply with this prohibition also after the termination of the legal relationship between me and the Controller.

……

(signature)

C. Model of the register of persons authorised to carry out the processing of personal data

No.	name, surname and position of the authorized person	Date of granting authorization	Date of expiring authorization	User ID	The scope of the authorization
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					

D. Model of designation of the Controller of the IT Systems

place, date ..... 20..... r.

The designation of the Controller of the IT Systems

Acting on behalf of the **Element spółka z ograniczoną odpowiedzialnością spółka komandytowo-akcyjna** with its registered seat in Gdynia, al. Zwycięstwa 96/98 lok. C1.04, 81-451 Gdynia, entered into the register of entrepreneurs maintained by the Regional Court Gdansk – North in Gdansk, 8th Economic Division of the National Court Register under KRS number 0000810330, Tax Identification Number (NIP) 5862349944, Statistical Number (REGON) 384697791, ("**The Controller**"),

I hereby appoint

Mr./Ms:.....

to perform the function of Controller of the IT Systems.

The specific responsibilities arising from this designation are set out in the Personal Data Protection Policy.

The designation is valid until revoked / to .....*

.....
(signature of the designator)

I declare that I accept the function of Controller of the IT Systems.

.....
(date and signature of the designated)

*delete as appropriate