PERSONAL DATA PROTECTION POLICY

(Privacy Policy)

FOR

SKYRISE SP. Z O.O.

Actualisation at February 2, 2019

DEFINITIONS

1. **Controller** (ADO) – means the controller of personal data, which is to be the Skyrise Ltd. (Sp. z o. o.), a company running business with registered seat at Jana III Sobieskiego Str. 2, 40-082 Katowice, being entered by District Court for Katowice, VIII Commercial Division within National Court Registry at number KRS 0000452810, having Tax Identification number (NIP) of 954-274-19-69 and Public Statistical Number (REGON) of 243196124, as a body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
2. **Personal Data** – means any information relating to identifies or identifiable natural persona („data subject") whereas 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;
3. **DPIA** – data protection impact assessment;
4. **Data Protection Officer (IOD)** – means a person pointed out by the Controller who coordinates execution of rules on personal data protection in relations to processing of personal data in Controller's organization;
5. **Third Country** - the country not being a part of the European Economic Area (EEA);
6. **Processor** – means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
7. **Personal Data Protection Policy** – herein document setting forth the rules of personal data protection under internal policy of the Controller;
8. **Employee** – a person who works within Controller's organisation under employment contract or othercivil law contract;
9. **Personal Data Processing** - means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
10. **GDPR** – the Regulation (Eu) 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 (General Data Protection Regulation);
11. **UE** – European Union;
12. **Personal Data Protection Act** – the legal act of 10 May 2018 on personal data protection (codification in Official Journal from 2018, issue 1000 with further changes);

I. ENTRY

Herein document of Personal Data Protection Policy give rise to rules and procedures of processing personal data protection in the organisation of the Controller. It provides with rules and guides on how personal data are managed and what are mechanisms of protection and giving the access to such data for entities in cooperation with the Controller.

By the virtue of herein Personal Data Protection Policy the given rules are to be implemented to all processing activities which are defined as such under GDPR. In particular, no matter the source of personal data, their scope, purpose of collecting, means of processing or timeline of processing, the rules given by this Policy need to be kept.

The rules of herein Policy are to be observed in any case the Controller is processing personal data as a controller within the meaning of GDPR, or such data are entrusted to the Controller for processing under personal data processing agreement or other legal act, or where personal data was made available to the Controller.

Organization structure in data processing activities

Responsible Entities

The Controller is responsible for personal data processing in its organisation and for protection of such data. According to GDPR and Personal Data Protection Act, in a date of adopting of herein Policy, the Controller is not obliged to appoint a data protection officer.

For protection and security of personal data, including managing the risk of keep the appropriate level of security and adopting control mechanisms, audits and preventive and corrective measures, the IT unit within the organisation of the Controller is responsible, president over by Employee: Łukasz Gruchala (lukasz.gruchala@skyrise.tech).

All considerations and questions or doubts in the area of personal data protection should be addressed by e-mail at it@skyrise.tech

Furthermore, the Controller shall indicate particular persons within the organisation being responsible for appropriate data protection while data processing activity as well as those empowered to take actions on personal data protection.

In the light of legal regulations, the Controller is liable in particular for:

- Implementation of appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with given rules on personal data protection (GDPR);
- Adoption of measures to permit the exercise of rights of data subjects;
- Maintaining records of personal data processing activities;
- Implementation appropriate policies and procedures;
- Keeping a registry of categories of personal data processing in the name of another controller under data processing agreement
- Cooperation with supervisory authority;
- Implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk of to the rights and freedoms of data subjects;
- Notification of personal data breach to supervisory authority as well as to communicate such to data subject, in prescribed cases;
- Giving the authorisation to Employees having access to personal data to process personal data and keeping records of such acts of authorisation;
- documenting any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken;

Persons authorised to personal data processing

Persons who has been authorised by the Controller to process personal data are committed to confidentiality under an appropriate statutory obligation of confidentiality and rules set forth in this document. Moreover, such authorised person is obliged to confidentiality for personal data as well as for measures and means of protection and safeguards.

In case of breach of obligation to protect personal data in respect of *inter alia* confidentiality commitments, the criminal liabilities are assumed notwithstanding that such follow for gross violation of basic duties of employee.

Structure of data in Controller's organisation software system

The Controller has ensured organised means of storing personal data within the software system being used in organisation (hereinafter referred to as "System"), in the scope of all data processed within Controller's organisation, including personal data.

The structure of data in the System takes into account all categories of data and their allocation in sub-systems, organised within the System for the internal purposes of Controller's organisation, including services outsourced from third entities as systems external to the System.

The Structure of data in in the System of Controller's organisation has been envisaged within Attachment no 1 to this Policy (document available under confidentiality).

II. GENERAL RULES FOR PERSONAL DATA PROCESSING

Principles relating to processing of personal data

Personal data are processed within the Controller's organisation with respect to the rules set forth in the Art. 5 of GDPR, i.e.:

- Lawfully – meaning within upon specific legal basis of processing provided by regulations under Art. 6 or Art. 9 of GDPR;
- Fairly – meaning within manner in in relation to data subjects' interests;
- Transparently – meaning within disclosure of details on the scope and the procedure of processing personal data to data subject;
- Limited to a purpose – meaning within specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Minimising data – meaning within adequate and relevant scope, limited to what is necessary in relation to the purposes for which they are processed;
- Accurately – meaning where necessary, kept up to date, ensuring that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified;
- Limited upon storage – meaning that personal data may 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;
- Upon confidentiality and integrity – meaning processed in a manner that ensures appropriate security of the personal data;

Scope of personal data processing

The protection is ensured for all personal data processed by the Controller without limitation to the form of such data (paper or electronic).

The list of series of data are provided within Attachment no 2 to this Policy (document available under confidentiality).

According to GDPR regulation the Controller shall maintain a record of processing activities under its responsibility.

That record shall contain all of information specified in Art. 30 GDPR, including the following:

- the name and contact details of the Controller and, where applicable, all joint controllers, as per specific category of data;
- the name of processing activity of internal body within Controller's organisation,
- the purposes of the processing,
- a description of the categories of data subjects and of the categories of personal data,
- legal basis of processing,
- where possible, the envisaged time limits for erasure of the different categories of data,
- categories of data recipients (other than processing entity),
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation;
- where possible, a general description of the technical and organisational security measures;
- whether processing activity requires data protection impact assessment – if so, indication of the location of a report from such assessment;
- the documentation of suitable safeguards

The abovementioned record has been run by the Controller in electronic form and falls under confidential information within the Controller's organisation, disclosed only in cases provided by legal requirements or provisions of contracts the Controller is a party to (specifically contracts under which the Controller is a processor of conferred personal data or contract under which the Controller conferred personal data processing to further sub-processors).

Specifically, the Controller ensures to make such record available to the supervisory authority on request.

Access of persons to processing personal data

The access to personal data within the internal Controller's organisation is to be granted only to a person, if acting under written, clear authorisation of the Controller given in advance, stored in System or by paper document, and who shall not process those data except on instructions from the Controller.

The authorisation to process personal data is granted to a person upon training or having familiarised in other form with rules of personal data protection enforced in the Controller's organisation, with a special impact to data which the authorisation relates to.

The authorisations to personal data processing are granted individually and point out data series to fall under such authorisation.

The form of authorisation with the confidentiality obligation of a person to be authorised and statement of getting familiar with rules of personal data protection is provided within Attachment no 3 to this Policy.

All authorisation given to personal data processing are registered in the Record of people authorised to process the data, kept by the Controller as provided within Attachment no 4 to this Policy (document available under confidentiality).

Outside the Controller's organisation, the access to processing personal data may be given falling under one of a situation:

1. Making available personal data (controller to controller);
2. Contracting personal data processing (controller to processor under contract)
3. Sub-processing personal data under further contract (the controller being a processor to sub-processor under further contract)

Making access to personal data

The Controller fallowing legal requirements and herein Policy regulation ensures that personal data to which acts as a controller **have been made available to other data collectors by access** in a proper form.

Access to personal data may be given only at least one legal basis of processing among those provided under Art. 6 of GDPR or under Art. 9 GDPR.

Entities or groups of entities/ persons whom personal data access have been made need to be registered within the Records of personal data processing kept by the Controller.

Delegating of personal data processing

The Controller fallowing legal requirements and herein Policy regulation ensures that delegation of processing personal data to which acts as a controller, may have been outsourced to third entity under a contract or other legal act subject to personal data processing, only if such processing is to take place within the purpose (and to the interest) of the Controller.

Before delegation of such processing to other entity acting as a processor, it is necessary to assess whether such satisfy legal requirements of proper personal data processing.

The Contract for processing personal data shall satisfy specifically requirements under Art. 28 of GDPR and shall stipulate:

- Subject-matter of processing
- Duration of processing
- The nature and purpose of the processing
- Type of personal data
- Categories of data subjects
- Requirements to sub-processing
- Obligations and rights of the controller
- Obligations and rights of the processor

The contract for delegation of personal data processing shall be in writing including in electronic form. Such contract for personal data processing shall be signed by authorised representative officer within the Controller's organisation or under given power of attorney.

Delegating the data processing under the contract shall be registered in processing activity Register kept by the Controller.

The Controller shall have the right to control and make audit of the entity to whom the processing has been delegated, as per rules of concluded contract on personal data processing.

The Controller may process personal data following from entities to whom the controller provides services. Access to and download of such data shall be preceded by concluding a contract on personal data processing and registration of such in registry of personal data processing record kept by the Controller.

Morover, as regulated by Art. 28 sec. 2 of GDPR, the processor shall not engage another processor without prior specific or general written authorisation of the controller. Detailed rules of allowed sub-processing shall be given in the contract on persona data processing or in any other document in written form, including electronic form.

Transfer of personal data to third countries

In case of transfer of personal data to a third country or an international organisation, it may take place where specific condition regulated in Chapter V of GDPR are fulfilled. Such specific conditions apply also to the data processor.

Transferring personal data to a third country or an international organisation may take the form of making personal data available or conferring the personal data processing. All such actions need to fulfil legal requirements and this Policy regulation.

Transfer of personal data to a third country or an international organisation may take place where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation

In case of lack of the Commission decision the Controller may transfer personal data to a third country or an international organisation provided that such entity proves to ensure an adequate level of protection and under the condition to respect human rights and fundamental freedoms as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred.

Adequate safeguards the Controller may ensure, without supervisory authority approval, by means of one of the following:

- legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules in accordance with egally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity;
- standard data protection clauses adopted by a supervisory authority and approved by the European Commission,
- an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights;
- an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights;

Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to as given above, the Controller may also provide for, in particular, by:

- contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

- provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

In the absence of an adequacy decision given by the European Commission or in case of lack of appropriate safeguards pursuant to what mentioned above, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards
- the transfer is necessary for the performance of a contract between the data subject and the controller
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person,
- the transfer is necessary for important reasons of public interest,
- the transfer is necessary for the establishment, exercise or defence of legal claims;,
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- the transfer is made from a register which is intended to provide information to the public

Joint controllers over personal data

Within activity taken by the Controller is allowed to take the joint controlling obligation towards personal data processing in cooperation to other entities.

Joint controlling over personal data shall take place where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.

It is allowable to act as such joint controllers in a provided that the three basic obligations are met:

- to be a data controller under regulation of Art. 4 GDPR;
- jointly determine the purposes of personal data processing;
- jointly determine the technical and organisational means of personal data processing .

Joint controllers shall mutually consult and determine in transparent manner respective responsibilities for compliance with the legal regulation of GDPR.

Information on processing personal data

Where personal data relating to a data subject are processed - in any case of processing personal data within the Controller's organisation - there is a need to provide data subject with information on such processing, in a form of Information Clause, according to regulations of GDPR.

- Information Clause for an employee – as provided by the Attachment no 5
- Information Clause for an worker under civil law contract – as provided by the Attachment no 6
- Information Clause for client (user of software Skyrise's software system) - as provided by the Attachment no 7

III. PROVISIONS ON SECURITY OF DATA PROCESSING

General rules of security and protection of personal data

1. In any case, only Employees within Controller's organisation have access to persona data based and provided they are properly authorised to processing such data.
2. Not authorised person remaining in the facility where personal data are processed may only be present therein upon the control and presence of a person having proper authorisation to personal data access.
3. Employees are committed to confidentiality over all information related to personal data being processed, including safeguards used and means of protections.
4. Employees are obliged to secure access to whatever documents and materials which may include personal data and to avoid access to such for unauthorised person. It is not allowed aslo to disclose any information related to personal data to other entities based on their application in whatever form (written, orally, or be phone or e-mail) without legal basis for processing personal data.
5. It is forbidden to taking any materials with personal data out of the area of authorised processing, especially if such is not related to performing Employee's duties.
6. Logins and passwords used to personalise an individual access by login into System of Controller's organisation or other system related to performing work may are not allowed to be disclosed to other person.
7. Sending e-mails to many person at one time needs to use UCC or BCC option (blind carbon option).
8. Employees are requested to obey the "clean desk" rule in their place of work under which no materials or documents with personal data are to be visibly stored on the desk, otherwiske allowing the access to personal data to unauthorised person. Drafts of documents, memo or copies of documents being out of use shall be in any case destroyed irrecoverably, e.g. with the use of document shredder.
9. In case of short breaks and absence at the place of work in Controller's organisation premises, during working hours and after, all Employees are obliged to close the room with a key in the area of places where personal data are processed.
10. After finished working within System in the Controller's organisation where personal data are processed, Employee is allowed to effectively log out from the System.

Audit for compliance of the personal data processing

Audit for compliance of data personal data processing is carried out by person appointed by Controller in order to examine technical and organisational measures used in Controller's organisation to verify whether those are compliant with legal requirements to personal data protection while processing activity.

Audit is to carried out once a year in first quarter by a person appointed by the Controller and having appropriate knowledge and competencies and based on the Controller's authorisation. Auditor shall provide with written report form the verification and compliance of personal data processing taking place in the Controller's organisation.

The form of authorisation to carry on the audit is provided within the Attachment no 8 to this Policy.

The person authorised to perform audit shall document activities taken within verification process to the extend necessary to assess the compliance of personal data processing with legal provisions on personal data protection.

Documentation may be provided inter alia by the export of data from the software system where personal data are processed or secured, loaded into data carrier or printout of such data as well as in a form of :

- taking notes from verification activities, specifically from gathered explanation and inspections, including reference to access to devices, dalta holders and software system where personal data is processed;
- Taking explanations form person which actions on personal data processing were under scrutiny;
- making copy of the document;
- making a copy of the screen of the device being a part of the software system used to process or safeguard personal data;
- making copy of a record from register of software system used for processing personal data or records of configuration of technical means of security systems;

Report from the audit should be prepared immediately after finalisation of audit activities – no later than within 1 month – and provides with among others:

- identification of the Controller and its registered seat;
- data and place of the audit;
- identification of the data protection officer (if such was appointed);
- list of activities taken by appointed auditor during the audit and identification of person participating in such audit activities;
- date of initialising and finalising of audit;
- scope and subject matter of the audit;
- description of factual background during the audit and other information relevant to assessment of the compliance of personal data processing with legal requirements;
- confirmed cases of personal data protection breach in the scope of audit, including planned or performed action to restore the breach;
- recommendation to develop personal data protection process or security upon processing of such data;
- list of appendixes being an integral part of the Report;
- signature of the appointed auditor.

Report may be provided in written form or electronic.

In case of remarks to the Report in respect of confirmed cases of breach, the Controller shall ensure taking immediate action to restore the breach towards compliance with legal requirements and to enforce precautions towards such breach in the future. After implementation of such, the Controller shall be given a report confirming lack of incompliance.

The person authorised to prepare after-audit report shall cooperate with the Controller till enforcing all necessary restoring actions and confirming lack of incompliance, which shall be issued in the same manner as the audit report within 30 days of time since audit has been finalised.

Data Protection Impact Assessment

The Controller for fulfilling GDPR requirements and by proof of satisfying the accountability obligation shall assess the impact on personal data protection in order to describe personal data processing and assessment, necessity and proportionality.

DPI Sheet form is provided within the Attachment no 9 to this Policy (document available under confidentiality).

.

Incident under personal data protection

The Controller Is committed to ensure security during personal data processing activities. In order to prevent from breach of personal data protection the Controller shall actively prevent from unauthorised access to premises and systems in the Controller's organisation, where personal data are processed as well as shall take actions against breach of personal data protection that already happened.

- In case of suspicion of the breach on the personal data protection has happened within the Controller's organisation the internal restoring procedure shall be initialised, aimed to take restoring actions and to eliminate the risk of breach of personal data protection.

  The Controller shall apply measures to action being taken according to the unified procedure as provided within Attachment no 10 to this Policy (document available under confidentiality).

- In case of personal data protection breach the Controller without undue delay – where feasible, not later than 72 hours after having become aware of it – notify such to the supervisory authority. In case of exceeding 72 hour term for notification the motifs of a delay shall accompanied the notification.

  Notification of the personal data protection breach shall comprise at least:

  - description of the nature of the breach, indicating the category and number of data subjects and category and number of records referring to data breach, as far as possible;
  - Identification of name and contact details of the data protection officer or identifying other point of contact from which more information may be achieved;
  - Description of possible consequences to data protection breach;
  - Description of measures taken or proposed to be taken by the Controller in order to prevent such date protection breach, in some cases the measures in order to minimalize possible negative effects of the breach;

The Controller may not provide with the notification in case the Controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The Controller shall document all personal data breach including the circumstances of personal data protection breach, its outcomes and actions taken to restore.

The form of the Register of cases of personal data breach or suspicion of such breach may have happened is provided within the Attachment no 11 to this Policy (document available under confidentiality).

Personal data subject rights performance

The Controller shall take into account within the structure of personal data process such prcedures and rules to facilitate data subject the performance of rights to which they are entitled under GDPR, including specifically:

- Right to withdrawal of given consent (Art. 7 sec. 3 GDPR),
- Right to access for personal data to data subject (Art. 15 GDPR),
- Right to rectification of personal data (Art. 16 GDPR),
- Right to erase personal data (right to be forgotten) (Art. 17 GDPR),
- Right to restriction of personal data processing (Art. 18 GDPR),
- Right to data portability (Art. 20 GDPR),
- Right to object (Art. 21 GDPR),
- Right not to be subject to a decision based solely on automated processing (Art. 22 GDPR).

Taking into account professional actions and appropriate performance of rights of person who has applied for the Controller to execute its right, the Controller has adopted unified internal procedure of actions for executing rights of personal data subject who has applied for performing its right as provided in Attachment no 12 to this Policy (document available under confidentiality).

Personal data data protection by design and data protection by default

The Controller takes into account personal data protection and privacy on every stage of creating and existing technologies falling over data processing. That means, the principles of privacy shall be "embodied" into any project assuming personal data processing, in such a way to give the effect that privacy protection exists as a part of that process at the very beginning.

Additionally, setting of software application or system where data are processed shall be designed to give protection by default and made access to only minimal information on the user.

When enforcing appropriate technical and organisational measures the Controller shall take into account:

- the state of the art;
- cost of implementation;
- nature, scope, context and purpose of data processing;
- the risk to the right and freedoms of data subject, of various likelyhood and severrity of that rist resulting from the processing wynikającego z przetwarzania.

Technical and organisation measures implied should ensure not to provide access to personal data to indefinite number of people.

The Controller proves that duties are performed by documenting appropriately among other in the form of e-mails, reports, notes or printout from the System.

.

Review and actualisation of this Policy

Person authorise be the Controller shall run through the regulation of this Policy once a year, verifying its adequacy towards factual process taking place in Controller's organisation and satisfying binding legal requirements on personal data protection area.

Performing such review it shall be taken the account:

1. outcomes of Repot from yearly audit;

2. recommendation followed from confirmed cases of personal data breach or threat of such breach of protection

Additionally, verification of this Policy shall take place in any case of amendments of personal data protection or in circumstances based on specific of the Controller' organisation.

Attachements:

1. Structure of data in in the System of Controller's - Attachment no 1
2. List of series of data - Attachment no 2
3. Form of authorisation with the confidentiality obligation of a person to be authorised - Attachment no 3
4. Record of people authorised to process the data - Attachment no 4
5. Information Clause for an employee – Attachment no 5
6. Information Clause for an worker under civil law contract – Attachment no 6
7. Information Clause for client (user of software Skyrise's software system) - Attachment no 7
8. Form of authorisation to carry on the audit - Attachment no 8
9. DPI Sheet form -the Attachment no 9
10. Internal procedures in Controller's organisation - Attachment no 10
11. Register of cases of personal data breach - Attachment no 11