PERSONAL DATA PROTECTION POLICY

in the company

“XOPERO SOFTWARE” S.A. (joint-stock company)
WITH REGISTERED OFFICE IN GORZÓW WLKP., POLAND

DOCUMENT’S VERSION:	**1.0**
EFFECTIVE DATE:	**05.02.2018**
NEXT VETTING DATE:	**05.02.2019**

DISCLAIMER:

This English version of Personal Data Protection Policy is established only for informational purposes. The binding version of this document is the Polish version.

CHAPTER I: POLICIES

I. THE AIM OF THE PERSONAL DATA PROTECTION POLICY

1. Personal Date Protection Policy was established in connection with requirements specified in Regulation (EU) NO 679/2016 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).

2. The definitions of the most important terms in this document are determined as follows:

   a) **Policy** or **PDPP** – this Personal Data Protection Policy

   b) **The Company** – shall be understood as XOPERO SOFTWARE with registered office in Gorzow Wlkp., Herbert 3 street, Gorzów Wlkp., postcode: 66-400, registered in Register of Entrepreneurs of the National Court Register under the KRS no. 0000684240, NIP no. 599-306-66-03, REGON(Official Business Register Number) No. 080285693.

   c) **Personal Data** – the information about identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

   d) **Processing** – 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

   e) **Filing system** – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis

II. THE ESSENTIAL PRINCIPLES

The Company introduces this Policy to inform that the personal data processed by The Company will 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 manner that is incompatible with those purpose;
c) adequate, relevant and limited to what is necessary in relations to the purpose for which they are processed;
d) accurate and, where necessary, kept up to date;
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 that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

III. CONSENT FOR THE PROCESSING OF PERSONAL DATA

1. Processing of personal data by The Company in the basic standard takes place based on a consent given by the person concerned.
2. The consent can be granted in writing as well as given by means of distance communication
3. The data subject has a right to withdraw his or her consent at any time. However, the withdrawal of consent shall not affect the lawfulness of processing performed based on the consent before the withdrawal.
4. The processing of personal data by the Company takes place within the scope necessary for the implementation of the contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.
5. The consent for having one's data processed can be granted only by the person who is of lawful age (above 18). On behalf of a person under 18, the consent shall be granted by his or her statutory representatives.

IV. OTHER BASES FOR DATA PROCESSING

The Company may process personal data also when:

a) 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;
b) processing is necessary for compliance with a legal obligation to which the controller is subject;

c) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
d) 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;
e) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a 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.

V. ACCESS TO PERSONAL DATA

1. The data subject shall have the right to obtain confirmation from the Company as to whether or not the personal data processed by the company concern the data subject , and, if that is the case, the data subject is entitled to have an access to the data and the following information:
    a) the purpose of the processing ;
    b) the categories of given personal data;
    c) information about the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular about recipients in third countries or international organizations;
    d) where possible, the planned period of personal data storage, or, if that is not possible, the criteria used to determine that period;
    e) where the personal data are not collected from the data subject, any available information as to their source;
    f) the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
2. The Company shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

VI. RECTIFICATION OF PERSONAL DATA

The data subject shall have the right to demand immediate rectification of any inaccurate personal data concerning him or her. Taking into account the aims of the processing, the data subject shall have the right to demand the completion of incomplete personal data, including by means of providing a supplementary statement.

VII. RIGHT TO ERASURE ('RIGHT TO BE FORGOTTEN')

1. The data subject shall have the right to request immediate erasure of personal data relating him or her and the Company shall have the obligation to erase personal data without undue delay where one of the following circumstances applies:
   - **a)** the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
   - **b)** the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing;
   - **c)** the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
   - **d)** the personal data have been unlawfully processed;
   - **e)** the personal data have to be erased for compliance with a legal obligation under European Union law or Polish law;
   - **f)** the personal data have been collected in relation to the offer of information society services.

2. Where the Company has made the personal data public and is obliged to erase the personal data in accordance to the above mentioned provisions, considering the available technology and the implementation cost, the Company shall take reasonable actions, including technical measures, to inform all the other Administrators processing the personal data that the data subject has requested that the Administrators erase any links to the data, copies of the data or their replications.
3. The Company will have the right to refuse the removal of all personal data or their parts if theirs processing is essential:
   - **a)** for exercising the right of freedom of expression and information;
   - **b)** for compliance with a legal obligation which requires processing under the law governing the Company;
   - **c)** for the establishment, exercise or defence of legal claims.

CHAPTER II: ESSENTIAL MATTERS

1. Persons engaged in the processing of the personal data

1.1. The Administrator of personal data

Name:	XOPERO SOFTWARE S.A.
Legal form:	joint-stock company
Tax Id. No. ***[NIP:]***	599-306-66-03
REGON:	080285693
National Court Register ***[KRS]*****:**	0000684240
Address:	ul. Herberta 3, Gorzów Wlkp., post code: 66-400

1.2. The person authorised to process personal data

The Company keeps records of persons authorized to process personal data with an indication of the purposes of the specific authorization and personal data files to which the authorization applies.

Records of persons authorized to process personal data are kept in writing and may also be kept in electronic form. Written form is attached as Annex 1 to the Policy (only in Polish language).

Authorization shall be issued and withdrawn by the Company's Management Board in writing. The authorization template is attached as Annex 2 to the Policy (only in Polish language).

1.3. Data Protection Officer (DPO)

DPO will be designated, as The Company processes personal data from many sources, providing services for the benefit of numerous parties, thus, the professionalization of issues concerning the protection of personal data is fully justified.

Data Protection Officer will be designated by the Board of The Company for the term of at least 2 years. DPO will directly report to the Board of The Company.

DPO will be immediately incorporated into all the affairs concerning the protection of personal data.

DPO will not receive any instructions concerning the performance of his or her task. They will not be dismissed or sanctioned for fulfilling their task.

Data subjects can contact DPO in all cases relating to the processing of personal data as well as exercising their rights.

DPO is obligated to maintain confidentiality with regard to the tasks performed.

The authorization template is attached as Annex 3 to the Policy (only in Polish language).

1.4. Processors

The Company may entrust the processing of personal data to another entity only by way of an agreement concluded in writing or electronically, in accordance with the requirements indicated for such agreements in art. 28 GDPR.

Before entrusting the processing of personal data, the Administrator, as far as possible, obtains information about the previous practices of the processing entity regarding the protection of personal data.

The list of processors with whom we cooperate is attached as Annex 4 to the Policy (only in Polish language).

2. The types of the personal data processed

The Company, in various situations, processes or can process the following types of personal data:

a) Name and surname,
b) Personal identification number;
c) Limited financial data;
d) Contact details: telephone numbers, e-mails, correspondence addresses etc.;
e) IP addresses.

It is not prohibited to process other data than only those indicated above, but each time it must be done either on the basis of the consent referred to in Section I point III or on one of the other grounds indicated in Section I point IV.

3. Personal data filing systems

The Company divides the personal data held and processed into filing systems that are created based on the key feature of the data subject, or the content of the system, or the method of obtaining data for a given system.

Only people authorized to process a given data filing system can have access to it.

The list of data filing systems is attached as Annex 5 to the Policy (only in Polish language).

4. Personal data storage and computer systems

As part of the processing of personal data, the Company will use the following data carriers:

a) Paper documentation;
b) Hard disks of various forms;
c) Mobile phones;
d) Flash drives;
e) DVD / CD discs.

IT systems and computer programs that are used or will be used:

a) Online mailboxes;
b) Web applications;
c) Cloud storages;
c) Office packages.

5. Rooms in which the personal data is processed

In terms of organizational and technical security, this Policy applies to the registered office of The Company and all real estate under the direct control of the Company.

The building where the rooms are located in which personal data is processed is under the 24-hour protection by a professional external entity (security company). The entrance door to the building is closed from 21:00 to 06:00 and the entrance key can be obtained only through security.

The building, its immediate surroundings and internal common parts (staircases, corridors) are covered by audio-visual monitoring. The recording from monitoring is stored for 30 days.

Within the premises occupied by The Company, the thematic sectors are separated, separated by walls and doors, with the possibility of locking. The sectors are as follows:

a) Office and administration department.
b) Technical department.
c) Development department.
d) Sales department.

The company has implemented a key management policy, which is aimed at limiting the availability of specific sectors only to authorized persons.

CHAPTER III: EMPLOYEES

This section is devoted to the special rules of personal data processing of employees. In the unregulated area, the provisions of Sections I and II of the Policy are applicable.

1. The type of workers' personal data

The Company processes the following types of employees' personal data:

a) Name and surname;
b) contact details;
c) identification number;
d) bank account number;
e) family data;
f) basic health data;
g) employment history
h) education,
i) interests.

2. The types of personal data sub-systems which include the workers' personal data

The Company divides the filing systems of employees data into sub-systems, which are created based on a distinctive key feature due to the content of this sub-system, or the method of obtaining data for a given sub-system.

Only people authorized to process a given sub-system can have access to it.

The following sub-systems were created in The Company:

a) Personal files,
b) Payrolls,
c) Lists of attendance,
d) Working time register,
e) Register of disciplinary penalties.

3. Workers’ personal data storage and computer systems

Additional IT systems and computer programs that are used or will be used in the processing of employees' personal data:

a) Płatnik;

4. **Rooms in which the workers' personal data is processed,**

Employees' personal data will be able to be processed as part of the office and administration department.

It is allowed to transfer the personal data of employees to a third party for processing - an external accounting or HR firm.

5. Activities of processing the workers' personal data

The list of the undertaken activities of processing along with their description:
a) Recruitment - downloading a CV questionnaire, cover letter, consent to the processing of personal data.
b) Employment - signing of the contract, preliminary medical examination, health and safety training, employee questionnaire.
c) Provision of work - verification of attendance, registration of working time, payment of salaries, payment of public and legal liabilities, supervision of employee duties, use of holidays.
d) Termination of work - issuance of a work certificate, payment of benefits due.

6. Recruitment

Recruitment takes place by placing an advertisement on a selected website.

Based on the documents sent, the candidates are pre-selected.

Selected persons are invited for interviews to the headquarters of The Company.

The conversation is conducted by the Board of Directors and the head of the department to which the recruitment is conducted.

It happens that after several job interviews candidates are invited for one more interview.

7. The description of activities related to the termination of employment relationship

After the termination of the employment relationship, a work certificate is issued immediately. Personal files are archived at the registered office of The Company. The e-mail account is deactivated, the access card is reprogrammed, data from the time recorder is deleted.

8. The documents required from the workers during the employment

Types of documents required from employees during employment:
a) Work certificates,
b) diplomas,
c) Certificates
d) Statements about family members subject to insurance applications
e) Medical certificate on the absence of contraindications to the work performed
f) Declaration on disability, affiliation to the NFZ branch, on subject to the Tax Office, on the willingness to exercise the right to care for a child, on familiarizing themselves with health and safety regulations, internal regulations.

Documents are completed in the administration department of the Company. After completing them, they are delivered to the HR department of the external HR company. In the human resources department, personal files are created and kept in paper form. Personal files are stored in the armored cabinet.

9. Maintaining the register of leaving the work place and the attendance list

The register of exits outside the workplace is kept in paper form and is located in the administration department.

The presence is confirmed by a magnetic card or magnetic key ring.
There are also personal paper attendance lists.

10. Pay slips

The pay slipss are clipped in a way that prevents reading without destroying them.
Disbursed individually only by an authorized person.

CHAPTER IV: THE IMPLEMENTATION OF THE OBLIGATIONS OF PERSONAL DATA ADMINISTRATOR

1. The forms of executing information obligations towards the data subject

Forms of providing information to the data subject:
a) On the website;
b) By writing
c) E-mail
d) Telephone.

2. The means of executing information obligations towards the data subject

Means of providing information provided for in the GDPR:

a) a special section on the website,
b) a dedicated document - an information card, available on the website and at the same time as downloading personal data and consenting to their processing.
c) in individual cases - personal, e-mail and telephone by the DPO.

3. The ways of obtaining authorization for processing personal data

Forms and methods of obtaining consent:

a) Electronic form.
b) Phone.
c) Paper form.

The withdrawal of consent to the processing of personal data may take place in any form from the above.

4. **The procedure of verification of the person reported**

Description of the applicant's identity verification methods:

a) In the case of a personal contact - a request to present an identity document, without the right to detain it or make a copy.
b) In case of distance contact - questions about characteristic and individual things for the account (e.g. login name, service name, project name, e-mail address)

5. The procedure for the recognition of applications related to the implementation of rights

Description of how to exercise the rights related to data protection:
a) Sending an application to the DPO.
b) Acceptance of the application.
c) Verification of the reporting person's identity
d) Consideration of the application - up to 30 days.
e) The possibility of extending the application deadline to 90 days
f) Decision making
g) Implementation of the decision

CHAPTER V: REISTERS AND RECORDS

1. The register of activities concerning the processing of personal data

The Company creates and maintains a register of personal data processing activities on an ongoing basis, which is attached as Annex 6 to the Policy (only in Polish language).

2. The register of personal data breaches

The Company creates and maintains a register of personal data breaches on an ongoing basis, which is attached as Annex 7 to the Policy (only in Polish language).

3. The register of persons authorised to process personal data

The Company creates and maintains a register of persons authorized to process personal data, which constitutes Annex 1 to the Policy (only in Polish language).

CHAPTER VI: SAFETY MEASURES

1. The measures of personal data protection other than the information systems

Appropriate locks
Magnetic access cards
Room access control system
Physically limited access to servers and network infrastructure
Physical protection
CCTV footage
Alarm systems
24/7 monitoring of the alarm signal
The restrictions in the access to codes disarming the alarm
Supervision over the keys to rooms
Supervision over the keys to the checkout
Closets, strongbox, safes
Clear desk policy
The correct setting of a monitor
The correct transfer of documents
Locked boxes for documents

2. The means of protection of the personal data in the information systems

The correct passwords policy
The separate badge for every user in the information system
Using the software allowing the creation of accounts
The blockade of giving the used badge to another person
The access granted after typing the access info
The access to the device granted after typing the login and the password
Limited access of the user to specified resources
Monitoring the users' access to some resources
Automatic logout after stated time of inactivity
The use of software tools
Testing of the quality of apps (code review, box scan, strength tests
weight measurement of system failings
Limiting interaction between the user and the system
Information audit
Antivirus software
Firewall
DMZ (computing)
Dispersed firewall
Proxy
DNS
Protection from phishing
Protection from Cross Site Scripting
Protection from Cross Site Request Forgery
Protection from SQL Injection
Using VNC, RConsole, TeamViewer (properly secured)
Regular updating software
Making the data backups
Making the programmes backups
Making the server backups
Standardization of the device
Standardization of the software
Pseudonymisation