Personal Data Protection Policy
at Centrum Finansowo-Księgowe EKKOM Sp. z o. o.
and its affiliates
dated 25 May 2018.

Having regard to the obligations resulting from Articles: 25 and 32 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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) (OJ L 119, p. 1), in order to ensure that all the personal data at **Centrum Finansowo-Księgowe EKKOM Sp. z o.o.** and its affiliates shall processed and secured in accordance with the applicable law by implementing the appropriate technical and organisational measures designed to effectively implement the data protection principles and provide such processing with all the necessary security measures and in order to ensure that personal data which is required to achieve each specific purpose of such processing shall be processed only by default.

Introductory provisions

1.1. The Policy shall define the principles of processing and securing Personal Data at the Company in order to ensure the convergence of such Processing with the requirements set in the GDPR and the applicable Polish law in the field of personal data processing. This policy shall form the grounds for all the requirements, procedures and principles of personal data protection implemented at the Company. The policy shall include
   (i) specification of the principles of data protection being binding for the Company;
   (ii) a set of procedures, instructions and detailed regulations on the processing of Personal Data at the Company and individual areas of personal data protection which constitute the Appendixes.

1.2. This Policy shall apply to all the Company staff and co-operators. This Policy shall also apply to all entities related with the Company, either in capital or in person. The list of all the related entities shall be contained in **Appendix No. 1.** The following units shall be accountable for ensuring that the Policy provisions are observed and kept:
   (i) the Company;
   (ii) the Company organisational units within which such Personal Data is processed;
   (iii) the staff.

1.3. The staff and co-operators employed by the Company or by any of its affiliates but posted to work at any Company's customer shall be first required to comply with the Customer's Security Policy and then to comply with this Policy and its provisions.

1.4. In order to effectively implement the Policy, taking into account the scope, context and objectives of the processing and the risk of infringement of the rights or freedoms of natural persons with its various probability and significance, the Company shall ensure:

(i) implementation of appropriate technical and organisational measures to ensure the compliance of Personal Data and its processing with the legal requirements and all the necessary security of Personal Data being processed;

(ii) permanent monitoring of the compliance of such processing of Personal Data with the legal requirements and keeping the measures referred to in Clause 1.4 (i) under constant review and updating;

(iii) control and supervision over the processing of Personal Data.

1.5. Such supervision over the compliance with this policy shall be ensured by the Company's Management Board. The supervision referred to in the preceding sentence shall be aimed in particular, but not exclusively, at ensuring that the activities related to the processing of Personal Data at the Company shall be consistent with all the legal requirements and the Policy provisions.

1.6. The Company shall ensure that the conduct of all Company's contractors, in particular its Processors and Co-Processors complies with the the Policy provisions in an appropriate scope at all situations where any Personal Data is transferred to such entities for its processing, including storage.

1.7. This Policy shall be stored and made available in a paper and electronic form at the Company's registered office.

1.8. The Policy shall be made available to:

(i) all the persons authorised to process Personal Data at the Company in order to provide them with appropriate knowledge and information on the principles and requirements concerning the processing of Personal Data at the Company – obligatorily;

(ii) the persons concerned, in particular any data subjects, at their request.

Glossary of terms

2.1. Whenever the following definitions or phrases are used in this Policy, they should be given the following meanings:

(i) Policy – this Policy and all its Appendixes, if any;

(ii) Personal Data – information on an identified or identifiable natural person, such as: his/her name, surname, identification number, location details, internet identifier or one or more factors being specific to his/her physical, physiological, genetic, mental, economic, cultural or social identity, as referred to in Article 4(1) of the GDPR;

(iii) GDPR – Regulation 2016/679 of the European Parliament and of the Council (EU) of 27 April 2016 on the protection of individuals 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) (O.J. EU L 119, p. 1);

(iv) Authorised person – any person authorised by the Company to process Personal Data within a given scope;

(v) Processing – an operation or set of operations performed upon Personal Data or sets of Personal Data, whether or not by automatic means, such as collection, recording, organisation, arrangement, storage, adaptation or alteration, download, retrieval, browsing through, use, disclosure by transmission, dissemination or otherwise making available, matching or merging, limiting, deleting or destruction, as referred to in Article 4(2) of the GDPR;

(vi) Data set – any structured set of Personal Data made available according to specific criteria;

(vii) Processor – a natural or legal person, public authority, entity or any other unit who/which processes Personal Data on behalf of the Company [e.g. IT service provider];

(viii) Co-Processor – a natural or legal person who/which processes Personal Data jointly with the Company on the basis of a close relation of Cooperation or other capital- or person-based relations.

(ix) Register – the Register of Personal Data Processing Activities at the Company;

(x) Authentication – an activity aimed to verify the User's declared identity;

(xi) Company – Centrum Finansowo-Księgowe EKKOM Sp. z o.o., address: 55 Krotoszyńska Street, 51-009 Wrocław, Tax Identification No. (pol. NIP): 8971668503, National Court Register No. (pol. KRS): 0000090054;

(xii) Affiliated companies –:

- Centrum Finansowo-Księgowe Ekkom Sp. z o.o. Sp. K., National Court Register No. (pol. KRS): 0000555876;
- Centrum Personalne EKKOM Sp. z o.o., National Court Register No. (pol. KRS): 0000615622;
- Centrum Personalne EKKOM Sp. z o.o. Sp. K., National Court Register No. (pol. KRS): 0000713627;

(xiii) Employees / Staff – persons employed at the Company on the basis of an employment relationship and natural persons cooperating with the Company on the basis of a civil-law contract;

(xiv) System – the System of personal data protection at the Company, referred to in Paragraph 5 of the Policy;

(xv) Sensitive data – the Personal Data referred to in Article 9 of the GDPR.

Personal data

3.1. The Company shall process Personal Data collected in data filing systems. The data filing systems processed at the Company shall be specified in **Appendix No. 2** to this Policy.

3.2. The list of Data Sets shall be updated or extended following a prior analysis of the effects and risks of such processing of personal data on the rights and freedoms of the individuals concerned.

3.3. The Company shall not undertake any Processing activities that could pose a significant risk of infringement of the rights and freedoms of any data subjects. In case of planning to undertake the activities referred to in the preceding sentence, the Company must conduct a prior assessment of the effects of such processing referred to in Article 35 of the GDPR.

3.4. By default, the personal data shall be processed within the area covering the Company's office premises located in Wrocław at 68a Robotnicza Street. Additional area at which the personal data is processed shall cover all portable computers and other data media located beyond the area indicated in the preceding sentence.

Grounds of Personal Data Protection at the Company

4.1. The Company shall ensure the application of technical and organisational measures required to guarantee the confidentiality, integrity, accountability and continuity of such Processed Data.

4.2. Authorised persons and all other persons to whom the Personal Data Processed at the Company is made available shall be obliged to process it in accordance with the legal requirements and the Policy provisions, as well as other internal legal acts in force at the Company or internal procedures related to the Processing of Personal Data.

4.3. When employing new Employees and in the course of employment, the Company shall ensure that:

(i) prior to commencing their duties, Employees shall be provided with appropriate knowledge on the principles and rules governing the Processing and protection of Personal Data at the Company;

(ii) each Employee shall be authorised in writing to process Personal Data to the extent necessary only, in accordance with the template set forth in Appendix no. 3 to this Policy;

(iii) each Employee shall be obliged to keep the confidentiality and integrity of Personal Data, in accordance with the template attached as **Appendix 4** to this Policy, with all the Staff being obliged, in particular, but not exclusively to:

(a) strictly comply with the scope of such authorisation;

(b) comply with the applicable legal requirements and the Processing Policy provisions;

(c) keep all the Personal Data secret;

(d) keep the confidentiality and integrity of methods of keeping Personal Data secret;

(e) immediately report to the Company about any incidents related to the breach of Personal Data and its security.

4.4. The Company shall ensure that the Personal Data Processed at the Company is:

(i) processed lawfully, reliably and transparently for its data subjects;

(ii) collected for the specified, explicit and legitimate purposes and not processed further when it is not inconsistent with these purposes;

(iii) adequate, relevant and limited to what is required for the purposes for which it is processed;

(iv) correct and, if necessary, kept updated; all reasonable steps must be taken to ensure that any personal data being incorrect in view of the purposes for which it is processed shall be immediately erased or rectified ("regularity");

(v) kept in a form which allows to identify the data subject for not longer than necessary for the purposes for which the data is processed;

(vi) processed in a manner which ensures an adequate level of its security, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, by means of appropriate technical or organisational measures.

4.5. While ensuring the Processing of Personal Data in accordance with the principles set forth in Clause 4.2 above, the Company shall base the Processing on the following grounds:

(i) Legality – the Company shall take care of privacy protection and process such Personal Data in accordance with the applicable legal requirements;

(ii) Security – the Company shall ensure an appropriate level of security of such Personal Data by constantly taking actions in this respect;

(iii) Individual rights – the Company shall enable persons whose Personal Data is processed to exercise their rights and it exercises these rights;

(iv) Accountability – the Company shall ensure due documentation on the manner it fulfils its obligations with respect to the protection of personal data.

4.6. In accordance with Article 37 of the Tax Advisory Act of 5 July 1996 (i.e. Journal of Laws of 2018, item 377, as amended), the Company shall take into account that the Personal Data processed in connection with the provision of tax advisory services is covered by the secrecy of a tax advisor. With respect to the Processing of Personal Data obtained in connection with the performance of activities under the secrecy of a tax advisor, the Company shall comply with the guidelines and requirements for professional secrecy.

4.7. The Company does not provide data subjects with information in case where such data must be kept confidential in accordance with the obligation of professional secrecy.

Personal data protection system

5.1. The Company shall ensure the compliance of Personal Data Processing with the legal requirements also by designing, implementing and maintaining the System. The System consists of organisational and technical measures in the field of protection being adequate to the level of risk identified for individual Data Sets and data categories. The System shall consist, in particular, of the following measures:

(i) access to the premises where the Personal Data is processed limited to the Authorised Persons only and ensuring that other persons may be present at the premises used for the Processing of Personal Data only at the company of such Authorised Person(s);

(ii) closure of the premises being the area referred to in Clause 3.4 of the Policy when the Employees are absent in such a manner as to prevent access to them by third parties;

(iii) guarantee that the area referred to in Clause 3.4 of the Policy is protected against random factors such as fire or flooding;

(iv) use of locked cabinets, drawers or other technical means to prevent unauthorised access to the Personal Data stored in them;

(v) implementation of the Clean Desk Policy, which is attached as **Appendix 5** to this Policy;

(vi) implementation of the Procedure for opening and closing the building and office premises, which is attached as **Appendix 6** to this Policy;

(vii) effective deletion or destruction of documents containing the Personal Data in a manner which prevents their subsequent retrieval;

(viii) assurance of hardware and information security, including:

(a) protection of the local network against externally-initiated activities,

(b) assurance of the validity of software used at the Company,

(c) protection of computer hardware used by the Company against malicious software,

(d) provision of permanent and frequent back-up of the data stored on all the Company computers, servers and the network,

(e) restriction of strict access to the Company hardware, software, server and local area network by applying authentication rules;

(ix) conduct of a risk analysis on all the data processing activities or data categories;

(x) implementation of the verification and selection standards for the Processors as well as the conditions for entrusting the Processing to individual Processors;

(xi) monitoring of changes in the Processing of Personal Data at the Company and on-going management of changes affecting the protection of Personal Data at the Company

Register

6.1. The register shall include categories of activities related to the processing of Personal Data at the Company Through the Registry, the Company shall record the processing of Personal Data and shall take stock of and monitor the manner in which it uses the Personal Data. The Register shall be attached as **Appendix 7** to this Policy.

6.2. Through the Register, in particular through the indication of general measures to be applied for the protection of Personal Data covered by a separate processing operation in

the Register, the Company shall also seek to demonstrate the compliance of the Processing of Personal Data with all the legal requirements.

6.3. The Register shall – separately for each identified category of operations in the field of the processing of Personal Data – record at least:

(i) name of a given operation;

(ii) purpose of such processing;

(iii) specification of the categories of persons whose Personal Data processed under the operation in question;

(iv) specification of the categories of Personal Data processed under the operation in question;

(v) legal grounds for such processing, including a specification of the category of a legitimate interest held by the Company, if the processing is based on such a legitimate interest;

(vi) specification of the categories of all the data recipients, including the Processors,

(vii) information on the potential transfer of Personal Data beyond the European Union or the European Economic Area;

(viii) general description of the technical and organisational measures for the protection of Personal Data applicable to the operation in question.

6.4. In the event of updating or broadening the category of Personal Data and its processing, the Company shall immediately update the Register in order to ensure its compliance with the actual standing and scope of such processing of Personal Data run at the Company.

6.5. The provisions of Paragraph 6.3 above do not exclude, if necessary, the possibility of including more information in the Register which increases its accuracy or legibility or which facilitates the compliance management of the protection of Personal Data with the legal requirements as well as the implementation of the principle of accountability.

6.6. In the Register the Company shall record the legal grounds for data processing for individual processing operations by indicating the general legal grounds for such processing, for example: its approval, agreement, legal obligation imposed on the Company and justified purpose of the Company.

Accomplishment of obligations towards Data Subjects

7.1. The Company shall implement consent management methods to enable their registration and verification of consents to process specific data for a specific purpose, consents for remote communication (e-mail, telephone, SMS, etc.) and registration of refusals to give such consents, their withdrawal and similar actions, such as filing objections or processing restrictions.

7.2. The Company shall take care of the legibility and style of provided information and communication with persons whose Personal Data is processed.

7.3. The Company shall publish the following documents on its website: www.ekkom.com.pl and make them available for inspection at the registered office of the Company:

(i) the Policy;

(ii) Information on the data subjects' rights;

(iii) Information on the scope of personal data processed for specific purposes;

(iv) Channels of contact with the Company with respect to personal data;

7.4. In order to exercise the data subjects' rights, the Company shall provide procedures and mechanisms to identify specific persons' data processed by the Company, integrate such data, make changes to it and delete it in an integrated manner.

7.5. By informing a given data subject concerned the Company shall make records on handling information obligations, notifications and requests:

(i) on the processing of his/her data when the data is collected from this person.

(ii) on the processing of his/her data, when this person's data is collected indirectly from him or her;

(iii) on the planned change of the purpose of processing of Personal Data.

(iv) prior to the revoking of any processing restriction.

(v) on the rectification, erasure or restriction of the processing of Personal Data (unless it would require disproportionate efforts or be impossible).

(vi) on the right to object to the processing of Personal Data at the latest at the time of the first contact with that this person.

7.6. The Company shall inform a given person without undue delay about any breach of personal data protection, if it is likely to cause a high risk to this person's rights or freedoms.

7.7. Irrespective of the provisions of Clause 7.5 above, the Company shall establish the method of informing persons on the processing of unidentified data, where it is possible (e.g. a plate informing that a given area is under video surveillance).

7.8. At the request of a given person regarding the access to his/her data, the Company shall inform this person whether it processes his/her data and about the details of such processing, in accordance with Article 15 of the GDPR, and shall provide this person with an access to the data concerning him/her. Access to the data may be granted by issuing a copy of such data.

7.9. The Company shall provide a Data Subject with a copy of Personal Data which relate to him/her and shall record that the first copy of such Personal Data was issued.

7.10. The Company shall rectify incorrect data at the request of its Data Subject. The Company shall be entitled to refuse to rectify any data unless a given person reasonably proves that the data to be requested is inaccurate. In the case of data rectification, the Company shall inform a given person on any recipients of such data at the request of this person.

7.11. When requested by a Data Subject, the Company shall supplement and update its data. The Company shall be entitled refuse to supplement the data if such supplementation is

inconsistent with the processing of Personal Data and its purposes. The Company may rely on a given person's statement as to the information supplemented, unless this statement is insufficient from the perspective of the procedures adopted by the Company, the law or there are grounds to believe that this statement is unreliable.

7.12. Subject to Clause 7.13 below, at the request of a given person, the Company shall delete Personal Data when:

(i) it is not necessary for the purposes for which it was collected or it is processed for other purposes,

(ii) its processing consent was withdrawn, and there is no other legal basis for its processing,

(iii) a given person lodged an effective objection to the processing of such data,

(iv) it was processed unlawfully,

(v) the need for its removal arises from any legal obligation,

(vi) this request relates to child's data collected on the basis of a consent in order to provide information-society services offered directly to this child.

7.13. When deleting Personal Data, the Company shall take into account to ensure the effective implementation of this right while respecting all the principles on data protection, including security, as well as verification whether there are no exceptions referred to in Article 17 Clause 3 of the GDPR.

7.14. If any data to be deleted was made public by the Company, the Company shall take reasonable steps, including technical measures, to inform other controllers processing such personal data that it is necessary delete the data and access to it. In case of data deletion, the Company shall inform a given person on all recipients of such data, at the request of this person.

7.15. The Company shall restrict the processing of personal data at the request of a given person when:

(i) this person contests the accuracy of such data – for a period of time required to verify its accuracy,

(ii) its processing is unlawful and the data subject makes an objection to the deletion of personal data (requesting ist restricted use instead),

(iii) The Company shall no longer need personal information, but it is necessary for the data subject to determine, pursue or defend his/her claims,

(iv) a given person objected to such processing on grounds related to his/her particular situation – until being determined whether the Company has legally justified grounds which override the grounds of objection.

7.16. Under restriction of data processing, the Company shall store data, but does not process it (does not use it, does not transfer it), without the consent of the data subject, unless to establish, pursue or defend claims, or to protect the rights of another natural or legal person, or for relevant public interest considerations. The Company shall inform this

person prior to lifting such restriction in the field of data processing. If data processing is restricted, the Company shall inform a given person on all data recipients, at the request of this person.

7.17. At the person's request, in a structured, commonly-used and machine-readable format the Company shall issue or transfer to another entity, if possible, data about this person provided by him/her to the Company, processed on the basis of this person's consent or in order to conclude or perform a contract concluded with him/her, at the Company's IT systems.

7.18. If a given person objects to the processing of his/her data referred to in Article 21 of the GDPR on the grounds of his/her special situation, and the data is processed by the Company on the basis of any legitimate interest of the Company or on the grounds of any task entrusted to the Company in the public interest, the Company shall undertake to take into account this objection, unless there are valid legally justified grounds for processing on the part of the Company, which prevail over the interests, rights and freedoms of the person submitting the objection, or grounds for establishing, asserting or defending claims.

7.19. If a given person objects to the processing of his/her data by the Company for the purposes of direct marketing, the Company shall consider this objection and discontinue such processing.

Minimisation of processed personal data

8.1. The Company shall implement procedures aimed to follow the principle of minimising the processing of Personal Data in terms of:

(i) adequacy of Personal Data for the purposes of Processing, including the limitation of the amount of Personal Data processed and the scope of such processing for the purpose of Processing;

(ii) restrict access to Personal Data to Authorised persons only, for whom the use of Personal Data to a specific extent is required for the proper performance of their duties;

(iii) limitation of storage time of Personal Data down to the period for which such storage of Personal Data is required to perform the purpose of Processing or the obligations imposed on the Company.

8.2. The Company periodically (at least once a year) reviews the amount of its processed data and the scope of such processing.

8.3. The Company shall apply restrictions on such access to Personal Information through:

(i) the Staff obligation to keep confidentiality, including with respect to Personal Data;

(ii) verification of a group of internal recipients of Personal Data by providing individual Staff members with specific privileges to process Personal Data;

(iii) implementation of logical technical measures to protect Personal Data by limiting access to all the systems, software and network resources used in the processing of Personal Data;

(iv) implementation of physical technical measures for the protection of Personal Data as indicated in Clause 5.1. (iv) Policies.

8.4. The Company shall update access privileges in the light of changes in the Staff composition and the roles of its members as well as changes in the processors. The Company shall periodically review the users entrusted at the Company's systems and update them at least once a year.

8.5. The detailed principles for physical and logical access control shall be set forth at the Company's physical and information security procedures.

8.6. The Company shall process personal data taking into account the criteria specified in the Register. The Company shall implement life-cycle data protection mechanisms at the Company, including in the field of verification of further usefulness and suitability of such data in relation to the deadlines and control points indicated in the Register.

8.7. Any data when its scope of usefulness is limited over time shall be deleted from the Company's systems as well as from handy and main files. Such data may be archived and stored on system-held and information back-ups processed by the Company. The Company's procedures in the scope of archiving, use of archives, creation and use of backups shall take into account all the data life-cycle control requirements, including the data erasure requirements.

Security of personal data

9.1. Taking into account the level of technical knowledge, implementation costs and the nature, scope, context and objectives of the processing of personal data as well as the risk of infringement of the rights or freedoms of natural persons with varied probability of occurrence and severity of such risk, the Company shall implement technical and organisational measures ensuring an adequate level of the protection of Personal Data which corresponds to the risk of infringement of the rights and freedoms of natural persons as a result of the processing of personal data by the Company.

9.2. The Company shall conduct and keep records on adequacy analyses of all the personal data security measures. In order to achieve it:

(i) The Company shall classify data and processing operations in terms of risks they represent;

(ii) The Company shall conduct risk analyses in the field of breaching the rights or freedoms of natural persons with regard to data processing operations or their categories. The Company shall analyse possible potential situations and scenarios of personal data breaches taking into account the nature, scope, context and purposes of data processing, risks of violation of the rights or freedoms of natural persons with varied probability of occurrence and severity of such risks;

9.3. The Company shall implement measures to ensure business continuity and prevent disaster effects i.e. measures to quickly restore the availability of and access to personal data in the event of any physical or technical incident.

Breaching the protection of personal data

10.1. In particular, but not exclusively, the following shall be considered an infringement or attempted infringement of the principles on the processing and protection of personal data:

(i) violation of the security of information systems in which Personal Data is processed;

(ii) provision of Personal Data to any unauthorised persons;

(iii) processing of Personal Data in breach of the set scope and purpose of its Processing;

(iv) unauthorised or accidental damage, loss, destruction or alteration of Personal Information.

10.2. In the event of a breach of the protection of personal data, the Company shall assess whether this breach may have resulted in a risk of infringement of the rights or freedoms of natural persons and shall estimate the scale of this risk.

10.3. In the event of a breach of the protection of personal data, the Company shall, without undue delay – if possible, not later than 72 hours upon this breach is identified – notify the competent supervisory authority of this breach, unless this breach is unlikely to result in a risk of breaching the rights or freedoms of natural persons. A template of the notification referred to in the preceding sentence shall be attached as **Appendix No. 8** to the Policy.

10.4. If risk of breaching the rights and freedoms of a given Data Subject is high, the Company shall also notify this Data Subject of the incident, unless:

(i) The Company shall implement appropriate technical and organisational protection measures and these measures shall be applied to the personal data to which this breach refers to and which prevent unauthorised reading of and access to such personal data;

(ii) The Company shall then apply measures eliminating the probability of high risk of violation of the rights or freedoms of this Data Subject; or

(iii) this would require disproportionately high efforts to take. In this case, a public communication shall be issued or a similar means shall be used by which this Data Subject is to be informed in an equally effective manner.

10.5. Irrespective of the obligations set forth in Clauses: 10.2-10.4 above, the Company shall keep records of all the personal data protection breaches, including their circumstances, effects and undertaken remedial actions. A template of the personal data breach register shall be attached as **Appendix No. 9** to the Policy.

Entrusting the processing of personal data

11.1. The Company may entrust the Processing of Personal Data to its Processor only by way of an agreement concluded in writing, in accordance with the requirements set forth in Article 28, Clause 3 of the GDPR. Such entrustment of the Processing of Personal Data, referred to in the preceding sentence may not lead to violation of the tax adviser's secret.

11.2. The Company shall engage only such Processors which give sufficient guarantees for the implementation of appropriate technical and organisational measures to ensure that the processing meets the requirements of this Regulation and to protect the rights of data subjects. In order to verify the fulfilment of the obligation referred to in the preceding sentence, the Company, prior to entrusting the processing to a potential processor, shall, as far as possible, obtain information on the principles of personal data protection applied by this potential processor, and on its practices regarding the protection of personal data.

Transfer of personal data to a third country

12.1. The Company shall not transfer Personal Data to a third country beyond the European Union or the European Economic Area, except at the request of the data subject.

12.2. In order to avoid any unauthorised export of such data, in particular in connection with the use of publicly available cloud services, the Company shall periodically verify the conduct of users and, if possible, shall provide equivalent solutions in accordance with the data protection law.

Final provisions

13.1. The Policy shall enter into force on the day of its announcement.

13.2. In case of matters not regulated by this Policy, the provisions of the GDPR and the generally applicable provisions of Polish and European law shall apply accordingly.

13.3. Any changes or additions to the Policy shall be made in writing in order to be effective, otherwise they shall be null and void. Amendments or additions to the Policy shall come into force not earlier than within 7 days from the date of their announcement.

13.4. The following Appendices, which form an integral part of the Policy, shall be attached to the Policy:

(i) Appendix No. 1 – List of entities related to the Company either in equity or in person;

(ii) Appendix No. 2 – List of Data Sets at the Company;

(iii) Appendix No. 3 – Template of Authorisation for the processing of personal data;

(iv) Appendix No. 4 – Template of Confidentiality statement;

(v) Appendix No. 5 – Clean Desk Policy;

(vi) Appendix No. 6 – Procedure for opening and closing the building and office premises

(vii) Appendix No. 7 – Template of Register of Processing Operations;

(viii) Appendix No. 8 – Template of Personal data breach notification;

(ix) Appendix No. 9 – Template of Register of personal data protection breaches;

Appendix No. 1 – List of entities related to the Company either in equity or in person

(i) **Centrum Finansowo-Księgowe EKKOM Sp. z o.o. Spółka Komandytowa;**
with its registered office at 55 Krotoszyńska Street, 51-009 Wrocław
with its place of business at 68a Robotnicza Street, 53-608 Wrocław
National Court Register No. (pol. KRS): 0000555876

(ii) **Centrum Personalne EKKOM Sp. z o.o.;**
with its registered office and place of business at 68a Robotnicza Street, 53-608 Wrocław
National Court Register No. (pol. KRS): 0000615622

(iii) **Centrum Personalne EKKOM Sp. z o.o. Spółka Komandytowa;**
with its registered office and place of business at 68a Robotnicza Street, 53-608 Wrocław
National Court Register No. (pol. KRS): 0000713627

Appendix No. 2 – List of Data Sets at the Company

Taking into account the definition in Article 4 Point 6 of the GDPR, the Company shall process Personal Data grouped in the following Data Sets:

(i) **Company's Employees** – covering personal data of natural persons employed at the Company on the basis of an employment contract (regardless of the grounds for its establishment), personal data of natural persons cooperating with the Law Firm on the basis of a civil-law contract (a commission contract, a contract for specific work) and personal data of apprentices and trainees engaged by the Company;

(ii) **Customers** – covering personal data of the Company's customers being natural persons, including persons running a sole proprietorship as well as personal data of natural persons being representatives of the Company's customers (members of management boards, proxies and attorneys of legal persons; their employees acting on behalf of contracting parties);

(iii) **Potential Customers** – covering personal data of the Company's potential customers being natural persons, including persons running a sole proprietorship as well as personal data of natural persons being representatives of the Company's potential customers (members of management boards, proxies and attorneys of legal persons; their employees acting on behalf of contracting parties);

(iv) **Suppliers** – covering personal data of the Company's suppliers being natural persons running a sole proprietorship as well as personal data of natural persons being representatives of the Company's suppliers (members of management boards, proxies and attorneys of legal persons; their employees acting on behalf of contracting parties);

(v) **Customers' employees** – covering personal data of the Customers' employees and co-operators serviced in the scope of HR and payroll by the Company;

(vi) **Customers' contracting parties** – covering personal data of customers and customers' suppliers serviced in the field of accountancy by the Company;

(vii) **Representatives of authorities** – covering personal data of representatives of the public administration bodies and common courts, the Supreme Court and administrative courts, acting on behalf of such bodies or courts;

(viii) **Unidentified data** – personal data not identified by the Company, such as data referring to persons monitored under the Company monitoring;

(ix) **Data in the case file** – personal data of natural persons processed in connection with procedures, inspections or court proceedings conducted by the Company (data referring to parties of such proceedings, their proxies, representatives, etc.).

Appendix No. 3 – Template of Authorisation for the processing of personal data

[Location], on [**Date**]

Staff authorisation to process personal data

Acting on behalf of [Company name], pursuant to Article 29 of Regulation (EU) of the European Parliament and of the Council (2016/679) dated 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46/EC (General Data Protection Regulation) (EU Official Journal L 119, p. 1) – hereinafter referred to as the GDPR – I grant:

[Name and surname of the authorised person]

employed as:

[Job position]

authorisation to process personal data in the scope of performed duties on the position held, i.e. you obtain authorisation to process personal data in the scope [Description of the scope of access to personal data, e.g. without restrictions, viewing personal data, data entering and processing, data removal].

The authorisation shall cover the processing of personal data:

(i) processed on paper media;
(ii) processed in IT systems:
  (a) [•],
  (b) [•],
(iii) Personal data covered by the Data Sets:
  (a) [•],
  (b) [•].

The authorisation shall include the right to process personal data in the period of employment.

At the same time, I oblige you to process personal data in accordance with the granted authorisation and with the provisions of the GDPR, the Act of [Date of the Act, upon its adoption] on the protection of personal data, the Labour Code, and the Employer's Personal Data Protection Policy.

At the same time, I authorise you to make/keep – for the purpose of your work – lists, records and registers of personal data, while keeping their full protection with the use of technical and organisational measures implemented at the Employer's premises.

Employer: _____

[Date and signature]

Appendix No. 4 – Template of Confidentiality Statement

[Location], on [Date]

Employee: [Employee's details]

Confidentiality commitment

I declare that – in connection with the performance of my official duties for [Company Name] and the authorisation granted to me to process personal data:

(i) I have been informed of the principles of processing and protecting your personal data in [Company Name], including:
   (a) the Personal Data Protection Policy dated [Policy Date],
   (b) all the procedures and regulations concerning the protection of personal data which bind the Company, including:
      – the Clean Desk Policy dated [Date of Adoption],
      – the Procedure for opening and closing the building and premises
   (c) all the provisions on the protection of tax advisor's professional secrecy
   (d) the rules of protection of personal data resulting from the provisions of mandatory law, in particular from the Regulation 2016/679 of the European Parliament and of the Council (EU) of 27 April 2016 on the protection of individuals 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) (O.J. EU L 119, p. 1);
(ii) the information and regulations referred to in Point (i) above and of the obligations imposed on me by the Policy is clear and understandable to me.

In view of the above, I shall undertake to

(i) immediately comply with the obligations imposed on me with regard to the protection of personal data;
(ii) ensure the protection, confidentiality and integrity of personal data processed in the data sets by the Company, in particular to ensure the adequate security of personal data against its disclosure or access (even accidental) to (by) third parties and unauthorised persons, as well as against its unauthorised or accidental damage, loss or modification,
(iii) keep secrecy and confidentiality of all the information processed in the course of employment at the Company, including upon cessation of works;
(iv) keep secret all the information on the operation of systems used to process personal data at the Company;

(v) immediately report any personal data breaches, as well as any observed attempts or facts of breaches in the security of premises or information systems to my superior.

Employer: _____

[Date and signature]

Appendix No. 5 – Clean Desk Policy

On 25 May 2018, Centrum Finansowo-Księgowe EKKOM Sp. z o.o. introduced the following Clean Desk Policy. This Policy shall apply to all the Company's Employees and co-operators.

The supervision over the policy and its implementation shall be entrusted to a person appointed for this purpose by the Management Board.

Clean Desk Policy

1. This Policy shall regulate the requirements and procedures for the protection of confidential data, including personal data processed at Centrum Finansowo-Księgowe EKKOM Sp. z o.o. and its affiliated companies by its Employees in paper form, including:
    a. paper documents;
    b. mail correspondence (letters);
    c. case files;
    d. source documents provided by the Company's customers;
    e. official correspondence.
2. Whenever the following definitions and phrases are used in the Policy, they should be given the following meaning:
    a. Policy – this Clean Office Policy and all its appendixes, if any;
    b. Employee – any natural person employed at the Company, or in its Affiliated Companies (by capital or by person), under an employment contract, as well as co-operating under a civil law contract (including within the scope of a sole proprietor's business activity), a student or school pupil who is not an employee of the Company in the course of an apprenticeship or internship;
    c. Company – Centrum Finansowo-Księgowe EKKOM Sp. z o.o. and related companies.
3. This Policy shall apply to all the Company's Employees, regardless of their position and time of employment with the Company.
4. Each Employee shall be obligated to limit restrict access to confidential data by third parties, including personal data contained on paper media used by this Employee in the course of his/her official duties.
5. In the course of work, each Employee shall be obliged to keep – on his/her desk or at his/her workstation – only documents which are required for this Employee to perform current tasks at the time of work. If such documents in question are no longer necessary for this Employee to conduct his/her current tasks, he/she shall be obliged to put them away. The provisions of Clause 6 below shall apply accordingly.
6. If an Employee leaves his/her desk or workplace – even temporarily – he/she shall be obliged to put aside all used documents containing confidential or personal data into a locked drawer or cabinet in order to prevent any third parties from accessing them.

7. If an Employee terminates his/her employment on a given day, prior to leaving the Company's registered office, he/she shall be obliged to perform the obligation referred to in Clause 6 below and to secure such documents against access by any third parties. When work is finished, there may be only a landline telephone and office accessories at the desk.
8. Employees must ensure that during their work at the workplace there are no liquids or other substances which could damage or destroy paper documentation when spilled. On the same grounds, an Employee shall be obliged to refrain from eating at the desk or at the workplace.
9. Notwithstanding the provisions of Clauses: 4-8 above, upon completion of work an Employee shall be obliged to put his/her official laptop in a lockable cabinet in order to prevent access to data stored on it by any unauthorised persons.
10. If any documents are no longer used by the Company as well as in cases specified in the Personal Data Protection Policy dated 25 May 2018, the Employee shall be obliged to immediately destroy such unnecessary documents in such a manner that it is not possible to reconstruct any information contained therein, unless the Personal Data Protection Policy dated 25 May 2018 provides another manner of their disposal or does not require them to be left or archived.

Appendix No. 6 – Procedure for opening and closing the building and office premises

On 25 May 2018, Centrum Finansowo-Księgowe EKKOM Sp. z o.o. introduced the procedure of opening and closing the building and office premises located at 68a Robotnicza Street in Wrocław, hereinafter referred to as "the Key Policy".

The supervision over the policy and its implementation shall be entrusted to a person appointed for this purpose by the Management Board.

Procedure for opening and closing the building and office premises

1) **Procedure for opening and staying in the building**
   a) The office premises located at 68a Robotnicza Street in Wrocław, hereinafter referred to as: the Premises shall be the place of business for Centrum Finansowo-Księgowe EKKOM Sp. z o.o.
   b) The persons indicated in the Appendix 1 to the Procedure shall be entitled to open and close the Premises.
   c) Upon opening the Premises and switching off the alarm system, the authorised person shall open the room where the lockable drawer with the keys to the other office rooms is located.
   d) At this room all the employees take the keys to their office rooms and acknowledge their receipt in the key register.
   e) In the absence of the persons holding the master keys to the building, a Member of the Management Board may authorise another employee to open and close the premises and office rooms.
   f) If it is impossible to open or close any building or office space, the employee shall immediately notify the Management Board Member accordingly.
   g) In office rooms, during working hours where there is only one employee, this employee shall be required to close the room each time he/she leaves it, excluding the rooms which are connected to other rooms with direct access to the corridor, provided that other employees are in the rooms.
   h) The staff may not stay at the Premises upon working hours of more than 30 minutes from the end of your work, except as provided in (i) and (j) below.
   i) Th staff may only stay at the Premises upon business hours or on holidays with the consent or written instructions given by their supervisor or, in the absence of the supervisor, his or her substitute.
   j) The following persons shall be exempt from the requirements set forth in letter h above.
      i) Members of the Management Board,
      ii) Team leaders,
      iii) other persons authorised in writing by a Member of the Management Board.
2) **Procedure for the activation and deactivation of alarm systems.**

a) The premises are subject to supervision and security consisting in 24-hour monitoring of the burglar alarm system / fire alarm system by the security company, in accordance with the principles set forth in the Agreement concluded with the entity.
b) The privileges to activate and deactivate the central alarm system shall be exercised by the authorised persons specified in Appendix No. 1 to the Procedure. Each of these people shall make use of an individual access password. Each time the system records the date, time and the person switching the alarm on and off.
c) The persons with access codes for the alarm system shall be obliged to exercise particular caution during their use. Such access codes shall be treated a business secret. The list of alarm codes shall be located in a safe, in a sealed envelope.
d) In the event of an alarm at the Premises, the guard company shall notify, in the sequence indicated, one of the persons listed in Part 3 of Appendix 1 to the Procedure. The task of this person is to enable the patrol service to enter the building (beyond office hours) and, depending on the circumstances, enable to enter the office premises in order to verify (and eliminate) any reasons for triggering an alarm.

3) Procedure for closing the building and rooms.

a) Upon completion of work, all the employees shall be obliged to close the premises using keys and record this fact in the Key Collection and Receipt Register (its template is attached as Appendix 2 to the Procedure).
b) The person listed in Appendix 1 to this Procedure shall be obliged to activate the alarm system. The alarm system shall be activated after checking the offices, corridors and sanitary rooms located in the Premises and determining whether it is possible to close the Premises.
c) The Premises shall be closed no later than at 4:30 PM. In justified cases, with the consent of a Member of the Management Board or any person replacing him/her, the closing time may be changed.

4) Procedure for the storage ad disposition of keys.

a) At Centrum Finansowo-Księgowe EKKOM Sp. z o.o., records are kept on the taking and collection of keys, in accordance with the template attached as Appendix 2 to the Procedure. The records are kept at the reception desk.
b) Keys to the Premises and offices shall be kept at the reception desk in a lockable drawer, excluding archive keys.
c) The persons in the possession of keys shall be obliged to adequately secure them against loss and theft and to keep records of entries to the Premises.
d) In the event of losing any key, getting it lost or finding its absence, an Employee immediately reports this fact to the Supervisor and, if necessary, in order to issue spare keys, submits a request to this effect.
e) The issue of spare keys to the employee may take place only in justified situations and when approved by a Member of the Management Board.

f) Spare keys for individual office rooms shall be stored in a metal box in the Secretary's office. The key to the spare key box shall be possessed by the persons listed in Appendix 1 to the Procedure.

g) The employees shall be prohibited from making their own copies of any keys to the Premises and offices.

h) It is forbidden to leave the keys in the door locks when a given employee is present / absent in the office room.

i) It is forbidden to make the keys available to unauthorised persons.

5) Authorisations

a) The persons listed in Appendix no. 1 – List of authorised persons to the procedure shall be granted appropriate authorisations to hold the keys. A template of the authorisation is attached as Appendix no. 3 – Template of the authorisation to hold the keys to the Procedure.

b) Such authorisations shall be attached to the authorisation binder, which shall be located at the Management Board Office.

6) Final provisions

a) The following Appendices shall be attached to the Procedure:

i) Appendix no. 1 – List of authorised persons;

ii) Appendix no. 2 – Records on the collection and return of keys to the office premises;

iii) Appendix no. 3 – Template of the authorisation to hold the keys

Appendix no. 1

to the Procedure for opening and closing of the building and office rooms

List of the authorised persons

Part 1 List of the persons permanently authorised to open and close the Premises

The following persons have permanent access to the Premises (they have an individual access code and a set of keys, including to open the key boxes):

(i) [•];
(ii) [•];
(iii) [•].

Part 2 List of the persons permanently authorised to open and close the Premises

The following persons have temporary access to the Premises (they have an individual access code and a set of keys, including to open the key boxes):

(i) [•];
(ii) [•];
(iii) [•].

Part 3 Persons notified in the event of an alarm

If an alarm is activated at the Premises, the security company shall notify the following persons:

(i) [•];
(ii) [•];
(iii) [•].

Appendix no. 2
to the Procedure for opening and closing of the building and office rooms

Records on the collection and return of keys to the office premises;

Key no.	*Key collection time*	*Legible signature of the person taking the key*	*Key return time*	*Legible signature of the person collecting the key*	*Remarks*

Appendix no. 3
to the Procedure for opening and closing of the building and office rooms

[Location], on [Date]

Authorization to hold the keys

Acting on behalf of [Company Name], I hereby authorise the following employee: [Employee's name and surname] to permanently/ temporarily hold a set of master keys to the Premises n the amount of [•] pcs as well as to have at the disposal an alarm code required to arm and disarm the Premises' alarm system.

The collection and return of the keys shall be documented in the Records on the collection and return of keys to the office premises.

The employee shall be obliged to properly secure the keys against loss and theft.

_____

[Date and signature of the Owner / Member of the Management Board]

I hereby confirm that I have got acquainted with the authorisation and the obligation as well as I have received the keys in the amount of [•] pcs., including:

(i) for the main doors – [•] pcs.,
(ii) for the alarm system box – [•] pcs.,
(iii) for the office rooms – [•] pcs.,
(iv) [•];

_____

[Date and Employee's name and surname]

Appendix No. 7 – Template of Register of Processing Operations;

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
No.	Name of processing operation	Organisational unit (department, division, etc.)	Purpose of Data Processing	Categories of people	Data categories	Legal basis	Data source	Data flow	Planned date of deletion of data categories (if possible)	Name of the co-controller and contact details (if applicable)	Name of the processor and contact details (if applicable)	Categories of recipients (other than the processor)	Name of the system or software	General description of the technical and organisational security measures in accordance with Article 32, Clause 1 (if possible)	Data Protection Impact Assessment (DPIA)	Transfer to any third country or international body	
																Transfer to any third country or international organisation (name of the country and entity)	If transfer and Article 49 Clause 1 Paragraph 2 – documentation on appropriate safeguards
			Article 30 Clause 1 Point b	Article 30 Clause 1 Point c	Article 30 Clause 1 Point c				Article 30 Clause 1 Point f	Article 30 Clause 1 Point a	Article 30 Clause 1 Point d	Article 30 Clause 1 Point d		Article 30 Clause 1 Point g		Article 30 Clause 1 Point e	Article 30 Clause 1 Point e
1.																	
2.																	
3.																	
4.																	
5.																	
6.																	
7.																	

Appendix No. 8 – Template of Personal data breach notification

[Location], on [Date]

[Company name]
[Company's address]
[Company's address]

President of the Office for Personal Data Protection
[Address of the body]
[Address of the body]

Reporting a personal data breach

Acting on behalf of the Company [Company name] with its registered office in [Registered Office], pursuant to the privileges granted to me and pursuant to Article 33, Clause 1 and 3 of Regulation 2016/679 of the European Parliament and of the Council (EU) of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (EU Official Journal L 119, p. 1), I hereby report the following personal data breach:

Controller of Personal Data and contact details of the breach:	
Date of the breach:	
Categories and approximate number of data subjects:	
Categories and approximate number of personal data entries affected by the breach:	
Describe potential consequences of the personal data breach:	
Describe the measures taken or suggested by the controller to remedy the personal data breach.	

_____

[Signature of the authorised person]

Appendix No. 9 – Template of Register of personal data protection breaches

No.	Description of the breach	Date of the breach	Category and number of people affected by the breach	Scope and/or categories of data affected by the breach	Circumstances of the breach – description of its nature, analysis of the event, reasons for its occurrence	Description of effects / consequences of the breach	Actions taken – a description of the measures taken or suggested to be taken to remedy the breach, including the measures taken to mitigate its negative effects	Result of the corrective actions