INFORMATION PROTECTION POLICY OF REMARK-KAYSER SPÓŁKA Z O.O. WITH ITS REGISTERED OFFICE IN BATOROWO

1) Protection strategy

§ 1 Definitions

1) The terms used in this Information Protection Policy shall mean:
   a) Data Controller – **REMARK-KAYSER SPÓŁKA Z O.O.**, with its registered office in Batorowo, REGON Statistical Id. No: 630689063, VAT Reg. No. (NIP): PL7811095831, subject to the provisions of Sec. 2 hereof,
   b) Employee – a person working for the Data Controller under an employment agreement or under other legally binding terms. The provisions of this Information Protection Policy referring to Employees shall also apply to interns and trainee Employees,
   c) Durable Medium – any material or tool that makes it possible to store information in a way enabling access to the information in the future for the period adequate to the purposes of such information, and to reproduce such information at any time in an unchanged form.
2) The provisions of this Information Protection Policy shall apply also if the Data Controller processes personal data as a processor entrusted with the data to be processed, or a processing entity in the meaning of the appropriate provisions of the law.

§ 2 Purpose

This Information Protection Policy is implemented for the following purposes:

a) ensuring the required involvement of Employees in maintaining the appropriate level of information security, including the protection of personal data processed by the Data Controller,
b) determining the directions of development of the information security management, including personal data protection, while complying with all requirements imposed by the applicable law, and maintaining smooth operation of the Data Controller,
c) identifying and reducing risks connected with information security, including personal data protection,
d) implementing the principles of compliance with the law, accuracy, clarity, purpose limitation, correctness, storage limitation, integrity, confidentiality and accountability of personal data processing.

§ 3 Formulation of the strategy of personal data protection

Data Controller safety is a condition determined by the adopted set of standards, principles, solutions, means and methods of information resource protection, measured by the level of risk of breach of accessibility, confidentiality or integrity of such resources. Data Controller safety is ensured when the risk of breach of accessibility, confidentiality or integrity of the Data Controller's protected resources does not exceed the acceptable parameters, while the principles determined in this Information Protection Policy and related documents are adhered to.

§ 4 General Regulations

In particular the following are subject to protection:

a) personal data processed by the Data Controller, regardless of their form and medium;
b) equipment used for processing, transferring and storing personal data by the Data Controller;
c) premises where key IT equipment containing personal data is housed;
d) documents and other durable media containing personal data;
e) software used by the Data Controller;

f) other property used or owned by the Data Controller;
g) information owned by contractors and external entities cooperating with the Data Controller – as part of such cooperation.

§ 5 Legal Framework

This Information Protection Policy is compliant with the provisions of the applicable law, in particular with:

- Regulation of the European Parliament and the Council (EU) on 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),
- the Polish Personal Data Protection Act of 10th May 2018,
- the Polish Act of 18th July 2002 on Providing Services by Electronic Means (Consolidated Text: Journal of Laws of 2017, Item 1219, as amended), if applicable to the particular case of processing,
- the Polish Telecommunications Law Act of 16th July 2004 (Consolidated Text: Journal of Laws of 2017, Item 1907, as amended), if applicable to the particular case of processing.

§ 6 Potential risks

The Data Controller's resources, in particular information and personal data, as well as the equipment necessary for their storage and processing, are of material importance to the Data Controller's business. In particular, the following categories of risks to Data Controller's resources are distinguished:

a) breach of confidentiality of data both by the Employees and persons not employed with the Data Controller, including by theft of resources,
b) loss of access to, or significant degradation of material functional parameters of the resource, or loss of data (destruction of resource) resulting from Force Majeure events or intentional/unintentional or accidental actions,
c) breach of data integrity as a result of unintentional, intentional or accidental actions,
d) implementation of inconsistent principles (standards, procedures) and means of systems' protection.

2) Organisation of the Data Controller's information protection

§ 7 List of data subjects and IT systems used to process such data

1) The Data Controller processes personal data grouped in the following categories (databases):
   a) Potential customers and contractors of the Data Controller; customers and contractors of the Data Controller;
   b) Employees and other persons employed by the Data Controller, former employees and potential employees and employed persons of the Data Controller.
2) Processed personal data categories (information fields):
   a) Full names,
   b) Addresses of residence, stay and office,
   c) Numbers from existing registers and records,
   d) Email addresses,
   e) Telephone numbers,
   f) Website addresses,
   g) Dates, places and scopes of products and services provided to the data subject by the Data Controller, or products and services in which the data subject expressed interest,
   h) Occupation or profession, education and qualifications of the data subject,
   i) Data on previous employment, experience and knowledge,
   j) Data on pension and other benefit rights,

k) Images in the form of photographs or records from an image-recording device,
l) Information on disabilities.

3) Personal data is processed in the following IT systems and applications:
– ERP Optima system,
– ERP XL system,
– Document Management system,
– Płatnik (ZUS) program,
– SYMFONIA program,
– MOZILLA THUNDERBIRD,
– MS EXCEL,
– MS WORD,
– MS POWERPOINT.

§ 8 Authorised Persons Register

1) The Data Controller may keep on a durable medium a "Register of persons authorised to process personal data", comprised of the following elements:
a) full names of the authorised person,
b) dates of granting authorisation,
c) dates of cessation of authorisation,
d) scope of authorisation,
e) identification of the authorised person (for data processed in an IT system),
f) signatures of the authorised person,
g) signature of the person making an entry in the register.
2) The register is updated and supplemented on a continuous and immediate basis, and an entry for a new person is only made when the requirements mentioned in §15 Sec. 3 are fulfilled.

§ 9 Protection Levels

1) Considering the categories of the processed data, the risks, and, in particular, the fact that the devices being a part of the IT system are connected to a public network, a unified high level of protection of personal data processing in the IT system is implemented.

§ 10 Processing data in the IT system

1) For each person whose personal data is processed in the IT system – excluding the systems used for processing personal data limited exclusively to text edition in order to make it available in writing – the system ensures the recording of:
a) the date of first entering the data into the system;
b) the identification of the user entering the personal data into the system, unless only one person has access to the IT system and data processing;
c) the source of the data, if not collected from the data subject;
d) information on recipients who were granted access to the personal data, the date and scope of such access, unless the IT system is used to process data contained in open databases.
2) The information mentioned in Sec. 1(a) and (b) hereinabove is recorded automatically after the user confirms the operation on the data.
3) For each person whose personal data is processed in the IT system, the system enables preparing and printing a report including information mentioned in Sec. 1 in a commonly readable form.
4) If the personal data is processed in at least two IT systems, the requirements mentioned in Sec. 1 may be satisfied in one of such systems or in a separate IT system used for that purpose.

§ 11 Safety measures

1) Safety measures implemented by the Data Controller including the high level:
A. Buildings, rooms or room sections where personal data is processed:

a) buildings, rooms or room sections where personal data is processed are protected from unauthorised access whenever the persons authorised to process personal data are not present;
b) presence of unauthorised persons in the area mentioned above is admissible subject to the Data Controller's consent or when accompanied by persons authorised to process personal data;

B. IT system:
a) in the IT system used for personal data processing, access control mechanisms are employed;
b) if access to the personal data processed in the IT system is granted to at least two persons, it is ensured that:
- the system registers separate identification for each user;
- access to data is only possible upon providing the identification and completing user authentication.
c) IT system used for personal data processing features protection, in particular from:
- software aimed at gaining unauthorised access to the IT system;
- loss of data caused by power failures or interference in the power supply network.
d) The IT system used for personal data processing is protected from risks associated with public networks by implementation of physical or logical security measures preventing unauthorised access.
e) The logical security measures mentioned above include:
- control of information flow between the IT system of the Data Controller and the public network;
- control of actions initiated from the public network and the IT system of the Data Controller.
f) The Data Controller uses cryptographic protection measures for the data used for authentication transferred within the public network.

C. User identification, backup copies:
a) identification of a user who has lost data processing authorisation may not be assigned to another person;
b) if passwords are used for user authentication, they must be changed at least once every 30 days. The passwords must be at least 8 characters long, contain uppercase and lowercase letters and a special character;
c) backup copies:
- are stored in places protected from unauthorised takeover, modification, damage or destruction;
- are deleted immediately after they cease to be useful.

D. Transport of devices containing personal data:
a) the person using a laptop computer containing personal data acts with particular care and attention when transporting, storing and using such a device outside of the buildings, rooms and room sections where personal data is processed, including using cryptographic protection measures for such personal data processed.

E. Procedure for handling devices, discs and other electronic storage media containing personal data:
a) devices, discs and other electronic information storage media containing personal data, intended for:
- destruction – are previously cleared off such data; if not possible, they are damaged in a way making them unreadable;
- handing over to an entity not authorised to process data – are previously cleared off such data in a way making their recovery impossible;
- repair – are previously cleared off such data in a way making their recovery impossible, or are repaired under the supervision of a person authorised by the Data Controller.

b) Devices and media containing sensitive personal data that are taken outside of the area, buildings, rooms and room sections where personal data is processed are protected in a way ensuring confidentiality and integrity of such data.

3) Personal Data Protection Officer

§ 12 Appointing a Personal Data Protection Officer

In accordance with the Data Controller's assessment, appointing a Personal Data Protection Officer is not required. A Personal Data Protection Officer will be appointed by the Data Controller if circumstances justifying appointing such an Officer occur.

§ 13 Reporting breaches of personal data protection

1) The Data Controller shall, without undue delay and where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2) The Data Controller shall, on a durable medium, document any and all breaches of personal data, comprising the circumstances relating to the personal data breach, its effects and the remedial actions taken. Such documentation shall enable the supervisory authority to verify compliance with this Article.

§ 14 Assessment of the processing impact on personal data protection and consultation

1) Where a type of personal data processing by the Data Controller – in particular using new technologies - due to its nature, scope, context and purposes, is highly likely to result in a high risk of breach to the rights or freedoms of natural persons, the Data Controller shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, as provided for in Art. 35 of the Regulation of the European Parliament and the Council (EU) on 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. A single assessment may be carried out for similar processing operations that present similar high risks.
2) The Data Controller shall prepare an assessment document mentioned in Sec. 1 on a durable medium. The assessment document shall contain at least:

   a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable (i.e. where not based on consent), the legitimate interests pursued by the Data Controller,
   b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
   c) an assessment of the risks of breach to the rights and freedoms of data subjects;
   d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
3) The Data Controller shall consult the supervisory authority, prior to processing, where an impact assessment for data protection indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller in order to mitigate the risk, as provided for in Art. 36 of the Regulation of the European Parliament and the Council (EU) on 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.

4) Obligations of Employees, Contractors and External Entities

§ 15 Obligations of Employees

1) This Information Protection Policy is binding for all Employees of the Data Controller. Any persons undertaking employment with the Data Controller and any other persons who acquire access to personal data accept the obligation to maintain the confidentiality of personal data accessed and the ways they are protected.
2) Each Employee who gains access to personal data is obliged, on the first day, to:
   a) read the principles, rules and provisions of this Information Protection Policy and confirm having done so by signing a declaration appended hereto as Attachment No. 1;
   b) complete a training on information security, including personal data protection, which is confirmed in the information security training sheet or in the Employee's declaration.
3) Access to personal data is granted to the Employee only subject to a written personal data processing authorisation and to signing of the declaration appended hereto as Attachment No. 1, and after entering such Employee in the register of persons authorised to process personal data mentioned in §8 hereof, if kept.
4) Employees of the Data Controller are entitled to use the personal data processed by the Data Controller solely for business purposes, unless otherwise required by specific regulations.

§ 16 Obligations of contractors and external entities

1) This Information Protection Policy is binding for all contractors, external entities and their employees, should they be granted access to the information resources of the Data Controller in the course of the performance of agreements.
2) If, in the course of the performance of an agreement, a contractor has or may be have access to the Data Controller's information resources, an information protection obligation clause is included in contractor agreements. Such a clause should contain the contractor's obligation to comply with this Information Protection Policy, to protect the information resources made available to the contractor by limiting their copying and sharing of such resources, and to return or destroy such resources upon termination of the agreement.
3) Material breach of information security by the contractor shall constitute basis for the Data Controller's withdrawal from the Agreement and for claiming compensation for any potential loss, or payment of contractual penalty, if provided for in the agreement concluded.

§ 17 Selecting processors or processing entities

The Data Controller only accepts the services of processing entities who provide sufficient guarantees of implementing adequate technical and organisational measures ensuring compliance of the processing with the requirements arising out of the law, and protection of the rights of data subjects.

§ 18 Necessary elements of an agreement

Every personal data processing agreement, processor or processing entity agreement concluded by the Data Controller must expressly state that the processing entity:

1) shall process personal data only upon documented instructions from the Data Controller - this applies also to transfers of personal data to a third country or an international organisation - unless required to do so by the Union or Member State law to which the processing entity is subject; in such a case, the processing entity shall inform the Data Controller of that legal obligation before processing, as long as that law does not prohibit granting such information on important grounds of public interest;
2) shall ensure that persons authorised to process the personal data have been obliged to maintain confidentiality or are under an appropriate statutory obligation of confidentiality;
3) shall implement all safety measures required by the law;

4) shall use only the services of the processors who provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the applicable law and ensure the protection of the rights of data subjects; and shall not engage the services of another processor without prior specific or general written authorisation. In the case of such a general written authorisation, another processor shall inform the Data Controller of any intended changes concerning the addition or replacement of other processors, thereby giving the Data Controller the opportunity to object to such changes;
5) taking into account the nature of the processing, shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Data Controller's obligation to respond to requests for exercising the data subject's rights;
6) taking into account the nature of the processing and the information available to the processing entity, shall assist the Data Controller in ensuring compliance with the obligations arising out of processing security, the obligation to report personal data breaches to the supervisory authority and to notify the data subject on personal data breaches;
7) at the choice of the Data Controller, shall delete or return all the personal data to the Data Controller after the end of the provision of services relating to processing, and deletes all existing copies thereof;
8) shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations imposed pursuant to the agreement, and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller. In connection with this, the processing entity shall immediately inform the Data Controller if, in its opinion, an instruction given to them infringes any provisions of the law concerning data protection.

Attachments to the Information Protection Policy:

1) Personal data processing authorisation template with employee declaration

_____ [Data Controller's representative body signature]
Document adopted on 25th May 2018