Table of contents:	Appendices:
1. Introduction	P-DG-14-01-z1 do Polityki ODO_Wzór upoważnienia do przetwarzania danych osobowych oraz zobowiazania poufnosci.docx P-DG-14-01-z2 do Polityki ODO_Wzór ewidencji upoważnień do przetwarzania danych osobowych.docx P-DG-14-01-z3 do Polityki ODOWykaz lokalizacji w których przetwarzane dane osobowe.docx P-DG-14-01-z4 do Polityki ODO_Procedura zgłaszania i oceny naruszeń.docx P-DG-14-01-z5 do Polityki_Zgłoszenie naruszenia ochrony danych organowi.docx P-DG-14-01-z6 do Polityki ODO_Zawiadomienie podmiotu danych o naruszeniu.docx PD-G-14-01-z7 do Polityki ODO_Rejestr czynności przetwarzania danych osobowych.xlsx PD-G-14-01-z8 do Polityki ODO_Rejestr kategorii czynności przetwarzania danych osobowych.xlsx P-DG-14-01-z9 do Polityki ODO_Rejestr Naruszen.xls P-DG-14-01-z10 do Polityki ODO_Zawiadomienie podmiotu danych o odbiorcach.docx P-DG-14-01-z11 do Polityki ODO_Informacja o niemożliwości zidentyfikowania.docx P-DG-14-01-z12 do Polityki ODO_Odpowiedź na żądanie podmiotu danych.docx P-DG-14-01-z13 do Polityki ODO_Informacja o przyczynie niepodjęcia działan.docx P-DG-14-01-z14 do Polityki ODO_Zawiadomienie podmiotu danych o przedłużeniu terminu.docx P-DG-14-01-z15 do Polityki ODO_Zawiadomienie podmiotu danych o uchyleniu.docx P-DG-14-01-z16 do Polityki ODO_Zawiadomienie odbiorców o zmian usunięc ograniczeniu.docx
2. Definitions	
3. Policy's scope and obligation to comply with it	
4. Policy availability	
5. Responsibility for policy	
6. Protection of personal data in the company – general principles	
7. Organisation of personal data processing by the company	
8. Method and scope of personal data processing	
9. Data protection system	
10. Inventory	
11. Registries	
12. Legal basis for the processing of personal data and their documentation	
13. Information obligations and the rights of data subjects	
14. Minimising and limiting the processing of personal data	
15. Security	
16. Reporting breaches of personal data protection	
17. Entrusting data processing	

DATA PROTECTION POLICY

WHEREAS:

1. Dr Gerard sp. z o.o. with its registered office in Międzyrzec Podlaski conducts a business activity consisting in the production of confectionery products (the '**Company**');
2. In connection with its business, the Company processes personal data of natural persons and is the controller of such data, and also, in certain cases, may be the entity processing the data on behalf of another controller (processor);
3. The Company is aware of the risks to privacy, including in particular the rights and freedoms of natural persons in relation to the processing of their personal data;
4. The Company complies with the requirements 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) ('**GDPR**'), including the requirement to implement appropriate organisational measures for the protection of personal data;

THE COMPANY ADOPTS THIS PERSONAL DATA PROTECTION POLICY

1. INTRODUCTION

1.1. The purpose of implementing this Data Protection Policy ('Policy') is to:

1.1.1. safeguard the personal data processed by the Company (this Policy constitutes an organisational measure for the protection of personal data within the meaning of Article 32 of the GDPR);

1.1.2. set out the principles for organising the protection of personal data, including maintaining the documentation required by the GDPR;

1.1.3. determine how the rights of data subjects whose data is processed by the Company are to be exercised;

1.1.4. determine the principles of performing the risk analysis related to the processing of personal data and the assessment of the effects of the processing on the protection of personal data;

1.1.5. determine the way the Company shall proceed in case of personal data protection infringements, including the management of such infringements;

1.1.6. determine the procedure to be followed in relation to the exchange of personal data with other entities.

1.2. This Policy consists of two parts:

1.2.1. a general part containing a description of the principles of personal data processing and protection applicable to the Company;

1.2.2. a detailed part containing appendices with additional procedures and document templates.

GENERAL PART

2. DEFINITIONS

Terms and abbreviations used in the Policy shall have the following meaning. Terms other than those indicated below that relate to the protection of personal data shall have the meaning given to them by the GDPR, unless otherwise expressly stated in this Policy.

Policy	this Data Protection Policy
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (Official Journal of the EU. L 2016 No 119)

personal data	information about an 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 the natural person, unless the context clearly indicates otherwise
special categories of personal data	data listed in Article 9(1) of the GDPR, i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for the purpose of uniquely identifying the natural person, or data concerning health, sexuality or sexual orientation
data relating to convictions and infringements	Personal data relating to convictions and infringements of the law (e.g. information on a criminal fine accepted by the Data Subject) or related security measures, the processing of which is permitted under Article 6(1) of the GDPR only under the supervision of public authorities or if permitted by Union law or Polish state law providing adequate safeguards for the rights and freedoms of Data Subjects. Any complete criminal conviction records shall be kept only under the supervision of public authorities
children's data	data of persons under 18 years of age
data subject	the person to whom the data relates
Controller	personal data controller, an entity which alone or jointly with others determines the purposes and means of the processing of personal data; for the purposes of this Policy the controller is the Company
Processor	a natural or legal person, or an organisational unit without legal personality, to whom the Company has entrusted the processing of personal data, and which the Processor processes on behalf of the Company (e.g. an entity which provides the Company with IT services, accounting services, document destruction services, HR and payroll services, marketing services) (processor within the meaning of Article 4(8) of the GDPR)
Recipient	natural or legal person, public authority, entity or any other body to whom personal data is disclosed, whether a third party (i.e. whether a natural or legal person, public authority, entity or subject other than the data subject, controller, processor, or persons who, under the authority of the controller or processor, may process personal data); however, public authorities that may receive personal data in the context of a particular proceeding in accordance with EU or Polish law are not considered recipients – the

	processing of personal data by these public authorities must comply with the data protection legislation applicable to the purposes of the processing; Examples of recipients: processor
supervisory authority	The President of the Office for the Protection of Personal Data or any other competent authority appointed to protect personal data in Poland or in another Member State of the European Union
processing	an operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automatic means, such as collection, recording, organisation, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data
joint controllership	the establishment of purposes and means of processing by joint agreement between two or more controllers, referred to as joint controllers
technical and organisational measures	measures to ensure an appropriate level of security of processing, e.g. pseudonymisation and encryption of personal data; the ability to ensure at all times the confidentiality, integrity, availability and resilience of the processing systems and services; the ability to restore rapidly the availability of and access to personal data in the event of a physical or technical incident; regular testing, measuring and evaluation of the effectiveness of technical and organisational measures to ensure the security of processing
profiling	any form of automated processing of personal data which involves the use of personal data to evaluate certain personal factors relating to an individual, in particular to analyse or predict aspects relating to the individual's work performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement
consent	a freely given specific, informed and unambiguous indication of the data subject's wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
breach of personal data protection	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed
international organisation	organisation and its subordinate bodies governed by public international law, or other body established by agreement between two or more States or on the basis of such an agreement
PDPS	A person holding a position of a personal data protection specialist in the Company

system	an IT system, i.e. a set of cooperating devices, software, information processing procedures and software tools used for the purpose of data processing
third country	country outside the European Economic Area
personnel	employees and associates of the Company, regardless of the basis of their employment
transfer of personal data	transfer to a third country or international organisation
Company	Dr Gerard spółka z ograniczoną odpowiedzialnością

3. SCOPE OF THE POLICY AND OBLIGATION TO COMPLY WITH IT

3.1. This Policy applies to personal data of natural persons, including in particular personal data of the Company's personnel members, job applicants, customers and potential and former customers of the Company, suppliers, agents as well as other natural persons whose personal data is processed by the Company.

3.2. The obligation to apply this Policy applies to all employees and permanent associates of the Company (regardless of their basis of employment) and suppliers. The Company shall, where possible, require associates and suppliers to comply with this Policy.

3.3. This Policy applies to the processing of personal data in a fully or partly automated manner (e.g. in IT systems, on computers) as well as in a traditional manner (e.g. in paper form) andregardless of whether personal data is or can be processed in datasets.

4. ACCESSIBILITY OF THE POLICY

4.1. This Policy is available online at the following link: the GDPR Procedure and in hard copy at the HR Department.

5. RESPONSIBILITY FOR THE POLICY

5.1. The Company's Board of Directors shall be responsible for the implementation and maintenance of this Policy.

5.2. Managers of each of the Company's organisational units are responsible for the implementation and maintenance of this Policy.

5.3. The PDPS is responsible for the supervision and monitoring of the compliance with the Policy.

6. PROTECTION OF PERSONAL DATA IN THE COMPANY – GENERAL PRINCIPLES

6.1. Pillars of personal data protection in the Company:

6.1.1. Legality – The Company is committed to protecting privacy and processes personal data in accordance with the law.

6.1.2. Security – the Company ensures an adequate level of security of personal data by taking continuous measures in this regard.

6.1.3. Rights of Data Subjects – the Company shall enable Data Subjects to exercise their rights and shall exercise those rights.

6.1.4. Accountability – the Company shall document how it fulfils its obligations in order to be able to demonstrate at any time the compliance of the processing of personal data with legal requirements.

6.2. Basic principles of personal data processing

6.2.1. The Company shall process personal data in accordance with the following principles and shall ensure that personal data is:

(a) processed lawfully, fairly and in a manner transparent to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes shall not be considered incompatible with the original purposes ('purpose limitation')

(c) adequate, relevant and limited to what is necessary for the purposes for which it is processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; the Company shall take all reasonable steps to ensure that personal data which is inaccurate in light of the purposes for which it is processed is erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data is processed; personal data may be kept for longer periods insofar as it shall be processed solely for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, provided that appropriate technical and organisational measures required under the GDPR are implemented to protect the rights and freedoms of data subjects ('storage limitation')

(f) processed in a manner that ensures adequate security of the personal data, including protection against unauthorised or unlawful processing

and accidental loss, destruction or damage, by means of appropriate technical or organisational measures ('integrity and confidentiality').

6.2.2. The Company shall be responsible for implementing the principles for the processing of personal data and must be able to demonstrate compliance with them ('accountability')

7. ORGANISATION OF PERSONAL DATA PROCESSING BY THE COMPANY

7.1. The Company as a controller

7.1.1. The Company shall perform the tasks of a controller with respect to the protection of personal data, such as:

(a) apply the basic principles of personal data processing in accordance with Article 5 of the GDPR;

(b) ensure that personal data processed by the Company is processed if at least one of the conditions referred to in Article 6(1) of the GDPR is met;

(c) take into account the protection of personal data at the design stage (*privacy by design* principle) and implement technical and organisational measures to protect personal data by default (*privacy by default principle*), in accordance with Article 25 of the GDPR;

(d) grant authorisations to process personal data within an appropriate, individually defined scope, keep records of the persons authorised to process personal data and other personal data protection documentation, and designate a person responsible for supervising this documentation, who shall be the PDPS;

(e) implement appropriate procedures in the event of a personal data breach or suspected personal data breach, including procedures for notifying such incidents internally within the organisation and for notifying the supervisory authority and the data subject of the breach;

(f) decide on the purposes and means of the processing of personal data, taking into account in particular changes in applicable law, the activities of the controller and the way in which it is organised, as well as the techniques for securing personal data;

(g) implement organisational and technical measures to ensure the security of personal data, and supervise the testing of their effectiveness and the updating of such measures;

(h) identify and verify the legal basis for sharing personal data with other entities;

(i) implement procedures for the identification of processors, the assessment of processors and the conclusion of agreements on the entrustment of the processing of personal data;

(j) conduct correspondence with the supervisory authority;

(k) prepare and approve document templates or appropriate clauses in personal data protection documents;

(l) ensure the improvement of the level of knowledge and awareness of the personnel regarding the processing and protection of personal data;

(m) fulfil the information obligations referred to in Articles 13 and 14 of the GDPR towards data subjects

(n) ensure the effective exercise of rights by data subjects;

(o) implement appropriate procedures and carry out a preliminary risk analysis related to new processes or projects involving the processing of personal data by the Company;

(p) implement appropriate procedures and carry out, prior to the start of processing, a data protection impact assessment of the intended data processing operations in accordance with Article 35 of the GDPR and, if necessary, consult the supervisory authority prior to the start of processing, if the data protection impact assessment referred to in the previous sentence indicates that the processing would entail a high risk;

(q) keep and update a register of processing operations as required by the GDPR.

7.2. Company as processor

7.2.1. The Company shall fulfil the obligations imposed on it as processor under the GDPR and the entrustment agreements and shall assist the controllers on whose behalf it processes personal data in complying with their obligations.

7.2.2. The Company shall maintain and update a register of all categories of processing activities carried out on behalf of other controllers.

7.3. Company personnel

7.3.1. The Company's personnel shall be obliged to:

(a) familiarise themselves with the principles of personal data protection, including the Company's internal regulations and participate in training courses organised or provided by the Company;

(b) comply with the Company's procedures, policies and guidelines aimed at lawful processing of Personal Data;

(c) provide the Company with the information and documents necessary to demonstrate that the Company has complied with its obligations under the personal data protection legislation;

(d) secure personal data against unauthorised access in accordance with the procedures in force at the Company, whereby this obligation applies both to data processed in paper and electronic form

(e) notify the Company, including the PDPS, of any cases indicating a suspected breach of personal data protection.

7.3.2. A breach of the principles set out in this Policy by a member of the Company's personnel, in particular deliberate disclosure of personal data to an unauthorised person, shall constitute a serious breach of fundamental duties of an employee / associate of the Company and may constitute grounds for termination of the employment contract without notice due to the fault of the employee or termination of the agreement with immediate effect in the case of persons other than the employee.

7.4. Authorisation to process personal data and duty of confidentiality

7.4.1. The Company, while implementing this Policy in the scope of providing access to personal data within its own (internal) structure, shall allow its processing in a computer system or in a paper form only to persons, who have obtained a prior appropriate authorisation to process personal data.

7.4.2. the authorisation is granted individually only to the extent necessary for the performance of duties by the person to whom the authorisation is granted. A template of the authorisation and the confidentiality commitment is attached as Appendix No 1 to this Policy.

7.4.3. The authorisation to process personal data shall be granted after the training (in traditional form, e-learning, by e-mail) on personal data protection has been carried out or the person is otherwise familiarised with the principles of personal data protection. The training referred to in the preceding sentence shall be conducted with particular attention to such issues as: (i) threats to information security, (ii) consequences of a breach of information security rules, including legal liability, (iii) application of measures to ensure information security, including devices and software to minimise the risk of human error.

7.4.4. The Company shall keep records of authorisations to data processing. The template of the register is attached as Appendix No 2 to this Policy.

7.4.5. The Company shall review authorisations.

7.4.6. Any person authorised by the Company to process personal data shall be obliged to protect such data in a way compliant with the provisions of this Policy. Such person is also obliged to keep the personal data and the ways of protecting it secret. This obligation exists also after termination of employment. The template of the confidentiality obligation is part of the authorisation template constituting Appendix No 1 to this Policy.

8. METHOD AND SCOPE OF PERSONAL DATA PROCESSING

8.1. Area of personal data processing

8.1.1. The Company shall process personal data at the Company's registered office and in other locations where the Company conducts its operations. A detailed list of locations where personal data is processed is attached as Appendix No 3 to this Policy.

8.2. Scope of data processing

8.2.1. In the course of its business, the Company shall, in particular, process data of the following categories of natural persons:

(a) Data of employees and co-workers (including data of former employees and co-workers) and temporary employees – this data is processed in electronic and paper form for purposes related to employment and the exercise of rights and obligations incumbent upon the Company;

(b) Job applicants' data – this data is processed in electronic and paper form for recruitment purposes;

(c) Customer data – this data is processed in electronic and paper form for purposes related to the performance of agreements, marketing, the assertion or defence of claims, the handling of complaints and grievances, customer satisfaction surveys and the improvement of service quality, as well as for the fulfilment of legal obligations by the Company;

(d) Data of business partners or representatives/contact persons of business partners (in the case of business partners other than natural persons) – this data is processed in electronic and paper form for the purposes of performing agreements, marketing, asserting or defending against claims, processing complaints and grievances, as well as for the purpose of fulfilling legal obligations by the Company;

(e) Data of customers and potential customers participating in competitions organised by the Company – such data shall be processed in electronic and paper form for the purposes related to the organisation and settlement of competitions organised by the Company and awarding and dispensing of prizes, as well as for the purposes of defence against claims or the assertion of claims related to competitions and for the fulfilment of legal obligations by the Company;

(f) Personal data of other categories of data subjects – before starting to process such data, the Company shall make an inventory in accordance with the provisions of point 9.1.1 of this Policy.

9. DATA PROTECTION SYSTEM

9.1. The Company's data protection system shall consist of the following elements:

9.1.1. Personal data inventory

(a) The Company shall identify on an ongoing basis the legal basis for the processing of personal data, the personal data resources held and their relationship to each other, the categories of personal data, the ways in which they are used (inventory), including:

a. cases of processing of special categories of personal data and data concerning convictions and violations of law;

b. processing of data of persons whom the Company does not identify;

c. processing of children's data;

d. profiling and automated decision-making which produces legal effects or significantly affects data subjects in a similar manner, e.g. targeting of offers on the basis of automatically analysed consumer choices;

e. data co-management.

9.1.2. Registers

(a) In order to comply with the accountability obligation, the Company shall keep:

a. a register of processing operations on personal data;

b. a register of all categories of processing operations carried out on behalf of another controller;

c. register of personal data breaches.

9.1.3. Legal grounds for the processing of personal data by the Company

(a) The Company shall ensure, identify and verify the legal bases for the processing of Personal Data, including:

a. The Company shall maintain a system for managing consents to the processing of personal data and remote communications;

b. The Company shall inventory and prepare a justification for cases where the Company processes personal data on the basis of a legitimate interest pursued by the Company or a third party;

c. The Company shall carry out a balancing test between the legitimate interests pursued by the Company or a third party and the rights and freedoms of the data subjects, which means that the Company, in situations of processing based on Article 6(1)(f) of the GDPR, i.e. if the processing is necessary for the purposes of the legitimate interests pursued by the Company or by the third party, shall assess whether the interests or the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child, are not overridden by those interests of the Company or the third party to justify the processing.

9.1.4. Compliance with information obligations towards data subjects

(a) The Company shall comply with the information obligations towards the data subjects referred to in Articles 13 and 14 of the GDPR and shall document the fulfilment of these obligations.

9.1.5. Fulfilment of data subjects' rights

(a) The Company shall ensure and review the possibilities and modalities for responding in relation to the exercise of data subjects' rights. The Company has implemented appropriate procedures to ensure that data subjects' requests are met within the timeframes and in the manner required by the GDPR, and are documented.

9.1.6. Minimisation and restriction of processing of Personal Data

(a) The Company applies the principles of managing the minimisation of Personal Data, such as:

a. verifying the adequacy of personal data for the purposes for which it is used before processing it;

b. restricting access to data to only those persons for whom such access is necessary;

c. identifying the correct period for the processing (including storage) of personal data and verifying its continued suitability for the purposes of the processing.

9.1.7. Security of personal data

(a) The Company shall ensure an adequate level of security of Personal Data by:

a. carrying out risk analyses for personal data processing activities or categories of personal data;

b. carrying out assessments of the effects of the processing of personal data on its protection in cases where the risk of infringement of the rights and freedoms of data subjects is high;

c. consulting the supervisory authority when required;

d. adapting personal data protection measures to the level of risk identified by the Company;

e. developing and implementing a procedure for the identification of processors, the evaluation and selection of contractors who will process personal data on its behalf (processors), as well as the requirements for the conclusion of personal data processing outsourcing agreements and the principles for verification of such agreements;

f. ensuring awareness of the Company's personnel regarding the principles and obligations related to the processing and protection of personal data.

9.1.8. Management of personal data protection breaches

(a) The Company has developed and implemented procedures to identify, assess and report an identified suspicion or data breach to a supervisory authority or a data subject, and has developed and implemented procedures to identify and report suspected or actual data breaches within the Company. The procedure for reporting personal data protection breaches is attached as Appendix No 4 to this Policy, the template for notification to the supervisory authority is attached as

Appendix No 5 to this Policy (with the proviso that if the law prescribes notifications to be made using official forms, the Company shall make such notifications using such official forms), the template for notification to the data subject is attached as Appendix No 6 to this Policy.

9.1.9. Processors / sharing of personal data with other controllers

9.1.10. The Company has developed and implemented procedures for evaluation and selection of processors, terms and conditions of personal data processing outsourcing agreements, as well as rules of conclusion and verification of the performance of outsourcing agreements. The processor evaluation procedure adopted by the Company and in force is available through the PDPS and at the address: GDPR Procedures

(a) Before sharing data with another controller, the Company shall verify the possibility of the transfer, including in particular its legal basis.

9.1.11. Transfer of personal data to a third country

(a) The Company, in connection with entrusting data processing to a processor, sharing personal data with other controllers or transferring personal data to an international organisation, shall (i) verify whether the Company shall transfer / transfer data to third countries and (ii) identify the legal basis for such transfer.

9.1.12. Application of *privacy by design* and *privacy by default* principles

(a) The Company, both when determining the means of processing personal data and during the processing itself, implements appropriate technical and organisational measures (e.g. pseudonymisation) designed to effectively implement data protection principles, such as data minimisation, and to give the processing the necessary safeguards to meet the requirements of the GDPR and to protect the rights of data subjects. In order to implement the above, the Company has developed and implemented a procedure for managing new projects / processes (including changes to existing projects / processes) affecting the privacy of data subjects. This procedure takes into account the need to assess the impact of the project / process on the protection of personal data, ensuring the privacy of data subjects (including having a legal basis, compatibility of the purposes of processing, security of personal data and its minimisation) already at the design phase of the process / project. The processor evaluation procedure adopted by the Company and in force is available through the PDPS and at the address: GDPR Procedures

(b) The Company has implemented appropriate technical and organisational measures so that, by default, only the personal data necessary to achieve each specific purpose of the Company's processing is processed. This obligation relates to the amount of personal data collected, the extent of processing, the period of storage and the availability of such data.

10. INVENTORY

10.1. Inventory

10.1.1. The inventory of new activities/new projects involving the processing of personal data shall include in particular the determination of:

(a) the type (category) of personal data (ordinary data, special categories of personal data, data relating to convictions and infringements);

(b) the purpose of the processing of personal data;

(c) the scope of personal data adequate to the purpose for which the Company shall process the personal data;

(d) the source of the data, i.e. whether the data comes directly from the data subject or from another source;

(e) the legal basis of the processing of personal data;

(f) the form of processing of the personal data (e.g. on paper, electronically);

(g) the period for which the personal data shall be processed;

(h) the recipients or categories of recipients of the personal data (including processors), as well as the legal relationship on the basis of which the transfer of the personal data to the recipients of the data takes place (entrustment of the processing of personal data to a processor / transfer of personal data to another controller / co-management of personal data).

10.2. Processing of special categories of personal data

10.2.1. The Company shall identify instances where it processes or may process special categories of personal data and shall maintain mechanisms to ensure the lawfulness of the processing of such data. In the event that instances of processing special categories of personal data are identified, the Company shall act in accordance with the accepted legal basis for processing in this regard.

10.3. Processing which does not require identification of the data subject

10.3.1. If, before or in the course of the processing of personal data, the Company determines that (i) the processing of personal data of data subjects is not necessary to achieve the purposes for which the Company processes the personal data of the data subject or (ii) that such processing of personal data is no longer necessary, the Company may not collect the personal data at all or delete the collected personal data, even if this affects the ability to comply with the provisions of the GDPR. Opting out of the processing of personal data is possible if the purposes for which the Company processes personal data do not require or no longer require (at all) the Company to identify the data subject.

10.3.2. In order to implement the above, the Company shall identify such cases, maintain appropriate documentation and, where applicable, inform the data subject of the non-identifiability.

10.4. Profiling and automated decision making

10.4.1. The Company shall identify cases of profiling, i.e. cases where the processing of personal data is: (i) carried out by automated means and (ii) serves to evaluate personal factors of data subjects, in particular to analyse (explicit profiles) or predict (predictive profiles) aspects concerning the data subject's performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement (e.g. analysis of the preferences of visitors to the Company's websites in order to formulate an offer for such visitors).

10.4.2. The Company shall also identify cases where a decision in relation to a data subject is based solely on automated processing of personal data by the Company, including profiling, and produces legal effects in relation to that data subject or materially affects the data subject in a similar manner.

10.4.3. Where cases of profiling or automated decision-making are identified, the Company shall act in accordance with the adopted principles in this regard, i.e. carry out data processing and maintain mechanisms to ensure the legality of this process.

10.5. Processing of children's data

10.5.1. The Company shall identify instances where it processes or may process children's data and shall maintain mechanisms to ensure the lawfulness of the processing of such data. Where processing of children's data is identified, the

Company shall act in accordance with the accepted legal basis for processing in this regard.

10.6. Joint controllership

10.6.1. The Company shall identify cases of joint controllership of personal data, i.e. cases in which at least two controllers (the Company and at least one other entity) jointly determine the purposes and means of personal data processing (which may occur e.g. in case of joint development and use of one IT system by these entities or in case of co-organisation of a competition or joint performance of the obligations under one agreement) and shall act in this respect in accordance with the adopted principles, i.e. the joint controllers shall, by means of a joint arrangement, clearly determine their respective responsibilities for the fulfilment of their obligations under the GDPR, in particular as regards the exercise of data subjects' rights and the exercise of information obligations towards data subjects. Irrespective of the content of the arrangements with the co-controllers, the Company shall ensure that the data subject can exercise their rights under the GDPR against the Company.

10.7. The implementation of the Company's obligations described in this point 10 shall be the responsibility of the managers of the Company's organisational units within which the processing of Personal Data takes place, who shall consult the PDPS to the appropriate extent in case of doubt.

11. REGISTERS

11.1. In order to fulfil the obligation of accountability, including documenting data processing activities by the Company, the Company shall keep:

11.1.1. a register of personal data processing activities in the Company (applies to personal data processed by the Company as a controller), in accordance with the template attached as Appendix No 7 to this Policy; this register shall be immediately updated with each new processing activity or other required information;

11.1.2. a register of all categories of processing activities performed by the Company on behalf of another controller (concerns personal data processed by the Company as processor), in accordance with the template constituting Appendix No 8 to this Policy; this register shall be immediately updated with each new category of processing activity or other required information;

11.1.3. a register of personal data protection breaches in accordance with the template constituting Appendix No 9 to this Policy; this register shall be

updated immediately after the receipt of information indicating a suspicion or a personal data protection breach regardless of the nature of such breach.

11.2. The company shall ensure that the records are available upon request to the supervisory authority.

11.3. The person responsible for keeping and updating the registers shall be the PDPS.

12. LEGAL BASIS FOR PROCESSING PERSONAL DATA AND ITS DOCUMENTATION

12.1. The Company processes personal data based on the legal bases set out in the GDPR. The Company identifies and verifies these grounds prior to processing.

12.2. The legal bases for processing personal data other than special categories of personal data (whereby 'special categories of personal data' are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and genetic data, biometric data for the purpose of uniquely identifying a natural person or data concerning the health, sexuality or sexual orientation of that person) and data relating to criminal convictions and infringements include, in particular, the following cases:

12.2.1. the data subject has consented to the processing of his/her personal data for one or more specified purposes; whereby, if the processing of personal data by the Company is to take place on the basis of consent, in the case of information society services offered directly to a child, the Company may process the personal data of a child who has reached the age of 16. If the child is under 16, such processing shall only be carried out by the Company where consent has been given or approved by the person with parental responsibility or custody of the child and only to the extent of the consent given. The Company shall, taking into account available technology, make reasonable efforts to verify that the person with parental responsibility or custody of the child has given consent or has approved it;

12.2.2. processing is necessary for the performance of an agreement to which the data subject is a party, or to take steps at the request of the data subject prior to entering into an agreement;

12.2.3. processing is necessary for the purposes of complying with a legal obligation on the Company as controller, i.e. when there is a provision of law which imposes an obligation on the Company as controller to process personal data;

12.2.4. the processing is necessary to protect the vital interests of the data subject or another natural person (vital interests are interests of great importance to the data subject or to another person, such as health and life, as well as property interests)

12.2.5. the 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 Company as controller;

12.2.6. processing is necessary for the purposes of 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 (e.g. processing of personal data for fraud prevention, marketing purposes or the assertion or defence of claims).

12.3. The GDPR establishes a general prohibition on the processing of special categories of personal data. The processing of special categories of personal data is only permitted where one of the following conditions is met:

12.3.1. the data subject has given his or her explicit consent to the processing of those personal data for one or more specific purposes, unless Union or Polish law provides that the data subject may not override the general prohibition on processing special categories of personal data;

12.3.2. processing is necessary for the purposes of complying with obligations and exercising specific rights by the Company or the data subject in the field of labour law, social security and social protection, insofar as it is authorised by Union law or Polish law, or by a collective agreement under the law of a Member State providing for adequate safeguards for the fundamental rights and interests of the data subject;

12.3.3. the processing is necessary to protect the vital interests of the data subject or of another natural person, and the data subject is physically or legally incapable of giving his or her consent;

12.3.4. the processing relates to personal data manifestly made public by the data subject;

12.3.5. the processing is necessary for the establishment, exercise or defence of claims;

12.3.6. processing is necessary for reasons of substantial public interest, based on Union law or Polish law, which are proportionate to the aim pursued, do not violate the essence of the right to data protection and provide for suitable and

specific measures to safeguard the fundamental rights and interests of the data subject;

12.3.7. processing is necessary for the purposes of preventive health care or occupational medicine, for the assessment of a worker's fitness for work, medical diagnosis, the provision of health care or social security, treatment or the management of health care or social security schemes and services on the basis of Union or Polish law or pursuant to an agreement with a health professional and subject to the worker being subject to the obligation of professional secrecy;

12.3.8. the processing is necessary for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes, on the basis of Union or Polish law, which are proportionate to the objective pursued, do not prejudice the essence of the right to data protection and provide for suitable specific measures to protect the fundamental rights and interests of data subjects.

12.4. The Company shall document the legal basis of data processing for individual processing activities.

12.5. When indicating a general legal basis for the processing of personal data (e.g. consent of the data subject, necessity for the performance of an agreement, performance of a legal obligation, protection of vital interests of the data subject, performance of public tasks, legitimate interest pursued by the Company or by a third party), the Company shall specify the basis in a clear manner when it is necessary, e.g. for consent – by indicating its scope, for legitimate purpose – by indicating a specific purpose, e.g. marketing of products or services, investigation or defence against claims. When processing special categories of data, the Company shall identify the relevant legal basis from Article 9 of the GDPR.

12.6. The Company shall update the implemented documentation on an ongoing basis and periodically review it at least once a year.

12.7. The implementation of the Company's obligations described in this point 12 shall be the responsibility of the managers of the Company's organisational units within which the processing of Personal Data takes place, who shall consult the PDPS to the appropriate extent in case of doubt.

13. INFORMATION OBLIGATIONS AND RIGHTS OF DATA SUBJECTS

13.1. General rules

13.1.1. The Company shall ensure that the provision of information and communication with Data Subjects is carried out in a concise, transparent, intelligible and easily accessible form, and in clear and plain language adapted to the categories of Data Subjects whose Personal Data the Company processes.

13.1.2. The Company shall ensure and facilitate data subjects' exercise of their rights under the GDPR through various measures, including: the provision of information in written form, orally (at the request of the data subject, provided that the Company confirms by other means the identity of the data subject), and electronically/documentally (e.g., sending by email or posting on the website information or links to information about data subjects' rights, how to exercise them with the Company and methods of contacting the Company, and requirements for identifying the data subject).

13.1.3. The Company shall ensure that the deadlines required by the regulations for fulfilling its obligations towards data subjects are met.

13.1.4. The Company has developed and implemented adequate methods of identification and authentication of data subjects for the purposes of fulfilling information obligations, providing notifications and exercising the rights of data subjects.

13.1.5. The Company shall document the fulfilment of information obligations, transmission of notifications, as well as responses to requests of data subjects, in particular, where possible, by obtaining from data subjects written confirmations of the transmission of relevant information and notifications.

13.2. Implementation of information obligations towards data subjects (Articles 13 and 14 of the GDPR)

13.2.1. The Company shall ensure the provision of information and fulfil its information obligations towards the Data Subject by means of appropriate information clauses/privacy policies covering at least the scope indicated in Articles 13 and 14 of the GDPR. The implementation of the Company's obligations described in this point 13.2 shall be the responsibility of the managers of the Company's organisational units within which the Personal Data is collected, who shall consult the PDPS to the appropriate extent in case of doubt.

13.2.2. The Company shall comply with the information obligation towards the data subject:

(a) in the case of collection of personal data from the data subject, at the time of collection (Article 13 of the GDPR);

(b) in case of collection of personal data not from the data subject (Article 14 of the GDPR):

a. within a reasonable period after the personal data has been collected – at the latest within one month of the date of collection (having regard to the specific circumstances of the processing of the personal data);

b. if the personal data is to be used for communication with the data subject – the information obligation should be fulfilled at the latest at the first such communication with the data subject, whereby (i) if the first communication with the data subject occurs before one month from the date of collection of the personal data, then the information obligation should be fulfilled at the latest with this first communication (even if the one month period has not yet expired)[1]; (ii) if the first communication with the data subject is to occur after one month from the date of collection of the personal data, then the information obligation should be fulfilled at the latest within one month from the date of collection of the personal data; or

c. if the personal data is to be disclosed to another recipient – at the latest upon its first disclosure, whereby (i) if the disclosure occurs within one month after the date of collecting the personal data, then the information obligation shall be fulfilled at the latest upon disclosure (even if the one month period has not expired yet); (ii) if the disclosure occurs after one month after the date of collecting the personal data, then the information obligation shall be fulfilled at the latest within one month after the date of collecting the personal data[2].

13.2.3. If the Company plans to further process the Personal Data for a purpose other than the purpose for which the Personal Data was collected, the Company shall, prior to such further processing, inform the Data Subject of that other

[1] *Article 29 of the Working Party Guidelines (version of 13 April 2018); accessed 23 April 2018.*
[2] *Article 29 of the Working Party Guidelines (version of 13 April 2018); accessed 23 April 2018.*

purpose and provide the Data Subject with all other relevant information required by the provisions of the GDPR.

13.2.4. The provision of the above information shall be free of charge.

13.3. Fulfilment of data subjects' rights

13.3.1. General Requirements

(a) In exercising the rights of Data Subjects, the Company shall apply procedural safeguards to protect the rights and freedoms of third parties. In particular, if the Company has reliable knowledge that the exercise of a data subject's request for a copy of personal data or the right to data portability may adversely affect the rights and freedoms of others (e.g. rights related to the protection of other persons' data, intellectual property rights, trade secrets, personal rights, etc.), the Company may ask the data subject to clarify the concerns or take other legally permitted steps, including refusal to comply with the request.

13.3.2. Data subjects' rights

(a) Right of access to personal data

At the request of the Data Subject, the Company shall confirm whether it processes the Data Subject's personal data, provide access to such data and provide the following information regarding:

a. the purpose of the processing of personal data;

b. the categories of personal data concerned;

c. the recipients or categories of recipients to whom the personal data has been or will be disclosed, in particular information about recipients in third countries or international organisations;

d. where possible, the intended period of storage of the personal data and, where this is not possible, the criteria for determining this period;

e. the right to request the Company to rectify, erase or restrict processing of the data subject's personal data, and to object to such processing;

f. the right to lodge a complaint with a supervisory authority;

g. if the personal data has not been collected from the data subject, any available information about its source;

h. automated decision-making, including profiling as referred to in Article 22(1) and (4) of the GDPR, and, at least in these cases, relevant information about the modalities of such decision-making, as well as the significance and the envisaged consequences of such processing for the data subject.

If personal data is transferred to a third country or an international organisation, the Company shall provide the data subject with the right to be informed of the appropriate safeguards referred to in Article 46 of the GDPR relating to such transfer.

The Company shall provide the data subject with a copy of the personal data undergoing processing. The provision of the first copy of the personal data shall be free of charge. The Company shall introduce and maintain a data copy price list, according to which it shall charge for subsequent data copies. The price of the data copy shall be calculated based on the estimated unit cost of handling a request for a data copy. If the data subject requests a copy by electronic means and does not indicate otherwise, the information shall be provided by commonly used electronic means. The right to obtain a copy shall not adversely affect the rights and freedoms of others.

(b) **Correction of personal data**

The Company shall rectify inaccurate personal data at the request of the data subject. The Company shall have the right to refuse the rectification of personal data, unless the data subject reasonably demonstrates the inaccuracy of the personal data requested to be rectified. In case of rectification of personal data, the Company shall inform the data subject about the recipients of the data, upon his/her request. A template of the notification is attached as Appendix No 10 to this Policy.

(c) **Completion of personal data**

The Company shall complete incomplete personal data at the request of the data subject. The Company has the right to refuse to complete the personal data if the completion would be incompatible with the purposes of processing the personal data (e.g. the Company may not process personal data that is unnecessary for the Company) The Company may rely on the data subject's statement as to the personal data to be supplemented, unless it is insufficient in the light of procedures adopted by the Company (e.g. as to the acquisition of such data), legal provisions or there are grounds to consider the statement unreliable. The Company shall inform the data subject about the data recipients upon his/her request A template of the notification is attached as Appendix No 10 to this Policy.

(d) **Deletion of data**

At the request of the data subject, the Company shall erase the personal data when:

a. the data is not necessary for the purposes for which it was collected or processed for other purposes;

b. the consent to its processing has been withdrawn and there is no other legal basis for the processing;

c. the data subject has raised an effective objection against the processing of such data;

d. the data has been processed unlawfully;

e. the necessity of erasure results from a legal obligation;

f. the request concerns the child's data collected on the basis of the consent referred to in Article 8 of the GDPR in order to provide information society services offered directly to the child (e.g. participation in a competition on the website)

In the event that personal data is made public, which the Company is obliged to erase in accordance with the above points, then, taking into account the available technology and the cost of implementation, the Company shall take reasonable measures, including technical measures, to inform the controllers processing such personal data that the data subject requests that such controllers erase any links to such data, copies of such personal data or replications thereof.

The Company has determined the handling of the right to erasure of personal data in such a way as to ensure the effective exercise of this right while respecting all data protection principles, including personal data security. The Company shall also verify beforehand whether any exceptions referred to in Article 17(3) of the GDPR apply (e.g. whether the processing is necessary for compliance with a legal obligation requiring the processing of personal data under Union or Polish law, or for the performance of a task carried out in the public interest, or for the establishment, exercise or defence of claims).

In case of erasure, the Company shall inform the data subject about the recipients of the data at his/her request. A template of the notification is attached as Appendix No 10 to this Policy.

(e) **Restriction of processing**

The Company shall restrict the processing of personal data at the request of the data subject when:

a. the data subject questions the correctness of the personal data – for a period allowing to verify the correctness of the personal data;

b. the processing is unlawful and the data subject objects to the erasure of the personal data, requesting instead the restriction of its use;

c. The Company no longer needs the personal data, but it are necessary for the data subject to establish, assert or defend claims;

d. the data subject has objected to the processing with – until it is established whether there are legitimate grounds on the part of the Company which override the grounds for the objection.

During the restriction of processing, the Company shall store the personal data, but shall not process (not use, not transfer) it without the data subject's consent, except in order to establish, assert or defend claims, to protect the rights of another natural or legal person, or for important reasons of public interest. The Company shall inform the data subject before the restriction of processing is lifted. In the case of a restriction of the processing of personal data, the Company shall inform the data subject about the recipients of the data, upon his/her request. A template of the notification is attached as Appendix No 10 to this Policy.

(f) **Portability of personal data**

At the request of the data subject, the Company shall issue in a structured, commonly used machine-readable format or transfer to another party, if possible, the personal data concerning that data subject which the data subject has provided to the Company, if the data is processed: (i) on the basis of the data subject's consent or (ii) for the purpose of entering into or performing an agreement concluded with the data subject, and the processing takes place in the Company's IT systems (by automated means).

(g) **Objection on grounds of the data subject's particular situation**

If the data subject raises an objection, motivated by his or her particular situation, to the processing of his or her personal data, and the data is processed by the Company on the basis of a legitimate interest of the Company or on the basis of a public interest task entrusted to the Company, the Company shall respect the objection, unless there are compelling legitimate grounds for the processing on the part of the Company overriding the interests, rights and freedoms of the objecting data subject, or grounds for the establishment, assertion or defence of claims.

(h) **Objection to direct marketing**

If the data subject objects to the Company's processing of their data for direct marketing purposes (including profiling), the Company shall respect the objection and cease such processing.

(i) **Right to human intervention in automated decision-making**

Where the Company processes personal data by automated means, including, in particular, profiling of data subjects, and consequently makes decisions in relation to the data subjects which produce legal effects or otherwise significantly affect the data subjects, the Company shall provide for the possibility of recourse to human intervention and decision-making on the part of the Company, unless such automated decision-making (i) is necessary for the conclusion or performance of an agreement between the data subject's data subject and the Company; or (ii) is expressly permitted by law; or (iii) is based on the express consent of the requesting data subject.

(j) **Objection for scientific, historical research or statistical purposes**

If the Company carries out scientific or historical research or processes data for statistical purposes, the data subject may raise an objection, motivated by his or her particular situation, to such processing. The Company shall respect such objection, unless the processing is necessary for the performance of a task carried out in the public interest.

13.3.3. Treatment of requests from data subjects

(a) If the Company receives a request from a data subject relating to the exercise of their right under the GDPR, the Company shall, before proceeding with the request:

a. verify the nature of the request and, if necessary, ask the data subject to provide additional information or clarification;

b. verify whether the data of the person (data subject) who submitted the request are processed by the Company;

c. verifies whether the data of the person (data subject) who submitted the request actually comes from that person (that data subject). If the Company has reasonable doubts as to the identity of the person (data subject) from whom the request originates, it

may request from such person additional information necessary to confirm his/her identity;

d. verify whether the request is feasible and whether there are no preconditions excluding the possibility of fulfilling the request (e.g. the Company may refuse to act on the data subject's request, if it demonstrates that it is not able to identify the data subject; a template of the information on the data subject's non-identifiability is enclosed as Appendix No 11 to this Policy);

e. verify the time and resources necessary to comply with the data subject's request.

(b) A template for responses to data subjects' requests is attached as Appendix No 12 to this Policy.

13.3.4. Deadline for complying with the data subject's requests

(a) The Company shall, without undue delay, and in any case no later than within one month of receiving the data subject's request, provide the data subject with information on the actions taken in relation to the data subject's request, including on the refusal to consider the request, on the reasons for not acting on the data subject's request, as well as on the possibility to lodge a complaint with the supervisory authority and to exercise remedies before a court, and on the data subject's rights relating thereto; A template for information on the reasons for not acting on the data subject's requests is attached as Appendix No 13 to this Policy;

(b) If necessary, the time limit referred to in point 13.3.4 (a) above may be extended for a further two months due to the complexity of the request or the number of requests. In this case, within one month of receipt of the request, the Company shall inform the data subject of such extension, stating the reasons for the delay. If the data subject has transmitted his/her request electronically, as far as possible, the information shall also be transmitted electronically, unless the data subject requests another form. A template for the data subject's notice of extension of the time limit for processing the request is attached as Appendix No 14 to this Policy;

(c) The extension of the deadline for fulfilling the data subject's request, as well as the refusal to take action, shall be agreed with the PDPS in each case.

13.3.5. Charges for the processing of data subjects' requests

(a) The fulfilment of data subjects' requests for communication and action pursuant to Articles 15-22 and 34 of the GDPR shall be free of charge. If the data subjects' requests are manifestly unfounded or excessive, in particular due to their continuing nature, the Company may:

a. charge a reasonable fee, taking into account the administrative costs of providing the information, conducting the communication or taking the requested action; or

b. refuse to act on the request.

(b) The Company has the obligation to demonstrate that the request is manifestly unfounded or excessive in nature. The refusal to act on the request, as well as the charging of a fee for complying with the data subject's request, will be agreed with the PDPS in each case.

13.4. Provision of other information

13.4.1. In order to comply with the information requirements of the GDPR, the Company shall:

(a) where possible, determines how to inform Data Subjects of the processing of de-identified data (e.g. a plaque that the area is covered by video surveillance);

(b) notify the data subject before lifting a restriction on processing; a template of the notification to the data subject on lifting a restriction on processing of personal data is attached as Appendix No 15 to this Policy);

(c) inform recipients of the rectification, erasure or restriction of the processing of personal data, unless this would involve a disproportionate effort or would be impossible; a template of notification to recipients of the rectification / erasure / restriction of the processing of personal data is attached as Appendix No 16 to this Policy;

(d) notify, without undue delay, the Data Subject of a personal data breach if it is likely to result in a high risk of harming the Data Subject's rights or freedoms; a template of notification of a personal data breach to the data subject is attached as Appendix No 6 to this Policy.

13.4.2. The provision of the above information shall be free of charge.

13.5. The implementation of the Company's obligations described in points 13.3 and 13.4 shall be the responsibility of the managers of the Company's organisational units within which the processing of Personal Data takes place, who shall consult the PDPS for each action before taking the action.

14. MINIMISATION AND RESTRICTION OF PROCESSING OF PERSONAL DATA

14.1. General comments

14.1.1. The Company shall ensure that the Processing of Personal Data is minimised in terms of: (i) the appropriateness of the personal data for the purposes (amount and type of personal data and scope of processing), (ii) access to the personal data, (iii) the duration of storage of the personal data.

14.2. Minimisation (restriction) of the scope of personal data processing

14.2.1. The Company has reviewed the scope and type of personal data acquired, the extent of processing, as well as the amount of personal data processed, in terms of adequacy of the purposes of processing as part of aligning its operations with the requirements of the GDPR.

14.2.2. The Company shall periodically review the amount of data processed and the scope of processing at least once a year. The review shall be performed within the Company by the head of the organisational unit where the documents containing personal data are kept.

14.2.3. The Company shall verify changes in the amount and scope of data processing under change management procedures (taking into account *privacy by design* and *privacy by default* principles).

14.3. Minimisation (restriction) of access to personal data

14.3.1. The Company shall apply access restrictions to personal data: (i) legal (confidentiality obligations, authorisation ranges), (ii) physical (access zones, locking of premises) and (iii) logical (restrictions of rights to personal data processing systems and network resources where personal data is stored)

14.3.2. The Company applies physical access control, in particular, it uses access cards, defines premises where documents containing personal data are stored and indicates persons who have access to such premises, ensures that keys to premises and cabinets where documents containing personal data are stored are not available to persons other than authorised).

14.3.3. The Company shall update access rights and authorisations upon changes in the composition of the personnel and changes in the roles of individual members of the personnel, as well as changes of the processors. Within the Company, managers of organisational units where documents containing personal data are stored in cooperation with the PDPS are responsible for updating access rights and authorisations.

14.3.4. The Company shall periodically review the granted authorisations to process personal data and update them at least once a year. The review shall be carried out within the Company by the head of the organisational unit in which documents containing personal data are stored in cooperation with the PDPS.]

14.3.5. The Company shall periodically review the established system users and update them at least once a year. The review shall be performed by the IT manager within the Company.

14.4. Minimisation (restriction) of the processing time of personal data

14.4.1. The Company has implemented mechanisms to control the life cycle of personal data in the Company, including verification of the continued relevance of personal data with respect to the deadlines indicated in the register of processing activities.

14.4.2. Personal Data, the processing of which has become inadmissible or unnecessary in relation to the purposes for which it was processed, shall be erased by the Company by:

(a) destruction of paper documentation;

(b) liquidation of equipment and media containing personal data;

(c) deleting personal data from IT systems;

(d) using the services of specialised entities offering services in the aforementioned areas.

Such data may also be anonymised in such a way that the data subjects cannot be identified at all or are no longer identifiable, but the anonymisation process must be irreversible.

15. SECURITY

15.1. General comments

15.1.1. The Company shall ensure a level of security appropriate to the risk of infringement of data subjects' rights and freedoms as a result of the processing of their personal data by the Company.

15.2. Raising awareness and knowledge on personal data protection

15.2.1. The Company shall ensure adequate knowledge of the Company's personnel on the principles of processing and protection of personal data and information security, internally or with the support of specialised entities, in particular by:

(a) providing data protection training to the Company's personnel, consisting in particular of: (i) initial training for new personnel members (in preparation for their work, e.g. in connection with the issuance of the authorisation referred to in point 7.4.3) covering at least the basic aspects of personal data processing arising from the provisions of the GDPR and national legislation, details of the processing activities in which a person will be involved in relation to the performance of their duties, the personal data protection principles applicable in the Company, the procedure to be followed in the event of a request by a data subject arising from the rights to which they are entitled under the GDPR or other personal data protection legislation, the characteristics of IT systems used to process personal data, including the principles of securing data processed in such systems; (ii) recurrent trainings for all personnel involved in the processing of personal data held at least once a year, (iii) ad hoc trainings – repeated or organised in case of significant changes regarding the protection of personal data in the Company;

(b) commitment of the Company's personnel to familiarise themselves with and comply with the provisions of this Policy;

(c) creation of a repository of documents relating to the principles of processing and protection of personal data in the Company and providing access to it for the Company's personnel.

15.3. Analyses

15.3.1. The Company shall categorise personal data and processing activities according to the risks they present.

15.3.2. The Company shall carry out analyses of the risks of infringement of the rights or freedoms of data subjects:

(a) for existing personal data processing activities in accordance with the activities registered under the register of processing activities – at least once a year;

(b) for new personal data processing activities – before the processing begins (preliminary risk analysis).

15.3.3. The Company shall analyse possible situations and scenarios of personal data protection breaches taking into account the nature, scope, context and purposes of the processing, as well as the risk of violation of rights or freedoms of data subjects with different probability of occurrence and seriousness of threat.

15.3.4. In performing the risk analysis, the Company shall determine in particular:

(a) what categories of personal data will be / are being processed (e.g. ordinary data, special categories of data, data relating to criminal convictions and infringements);

(b) whether profiling will take place, including its use for marketing purposes;

(c) whether automated decision-making which produces legal effects or has other similar significant effects on the rights and freedoms of data subjects will take place;

(d) whether there will be systematic monitoring (e.g. processing of personal data to observe, monitor or control data subjects; video surveillance, monitoring of computer systems);

(e) whether personal data will be processed on a large scale;

(f) whether data relating to vulnerable persons, e.g. children, elderly, employees, will be processed;

(g) whether new technological or organisational solutions will be used;

(h) whether the processing itself prevents data subjects from exercising a right or benefiting from a service or an agreement;

(i) what are the feasible measures to protect personal data, including organisational and technical security measures (e.g. pseudonymisation, encryption of personal data, other cyber security measures comprising the ability to continuously ensure the confidentiality, integrity, availability and resilience of processing systems and services, business continuity and disaster prevention measures, i.e. the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident), and assess the cost of their implementation;

(j) whether and how high the risk is that unauthorised third parties will gain possession of or access to the personal data;

(k) what are the possible consequences of a personal data breach for the Company, data subjects and third parties.

Depending on the results of the analysis, the Company shall determine whether a data protection impact assessment should be carried out.

15.3.5. The Company's adopted and applicable template of the procedure for risk analysis and assessment of the effects of the processing on the protection of personal data is available through the PDPS and at the address: GDPR Procedures.

15.4. Assessment of the effects of the processing on the protection of personal data

15.4.1. Where, as a result of the risk analysis referred to above, it is determined that a risk is, or is likely to be, high, the Company shall assess the effects of the intended processing operations on the protection of personal data in cases where, according to the risk analysis, the risk of infringement of the rights and freedoms of data subjects is high. When making such an assessment, the Company shall consult with the PDPS.

15.4.2. A personal data protection impact assessment shall be required in particular in case of:

(a) a systematic, comprehensive assessment of personal factors relating to data subjects which is based on automated processing, including profiling, and is the basis for decisions which produce legal effects on the data subject or similarly significantly affect the data subject; or

(b) the large-scale processing of special categories of personal data, data relating to criminal convictions and infringements; or

(c) the systematic large-scale monitoring of publicly accessible sites.

15.4.3. Before carrying out a data protection impact assessment of the processing, the Company shall also verify whether the processing operation for which such assessment is to be carried out is on the list of operations mandatorily subject to such assessment or on the list of operations not subject to such assessment published by the supervisory authority. In this respect:

(a) if the planned operation is on the list of operations mandatorily subject to assessment – the Company does not carry out an analysis of whether it is necessary to carry out an assessment of the effects of the processing on the protection of personal data, but instead carries out an assessment of the effects of the processing on data protection;

(b) if the planned operation is on the list of operations not subject to assessment – the Company shall not carry out an assessment of the effects of the processing on the protection of personal data, unless the planned operation, in the opinion of the Company, carries a likelihood of

a risk of infringement of the rights or freedoms of data subjects to the extent justifying the necessity to carry out an assessment of the effects of the processing on data protection.

15.4.4. The assessment of the effects of the processing on the protection of personal data shall contain at least (in the form of a written report):

(a) a systematic description of the intended processing operations and the purposes of the processing, including, where applicable, the legitimate interests pursued by the Company;

(b) an assessment of whether the processing operations are necessary and proportionate in relation to the purposes;

(c) an assessment of the risk of a breach of the rights or freedoms of data subjects; and

(d) the measures planned to address the risk, including safeguards and security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of data subjects and other affected persons.

15.4.5. Where necessary, and at least when the risks arising from the processing operations change, the Company shall conduct a review to determine whether the processing is carried out in accordance with the assessment of the effects of the processing on the protection of personal data.

15.4.6. The Company shall conduct and document analyses of the adequacy of personal data security measures.

15.4.7. The Company's adopted and applicable template of the procedure for risk analysis and assessment of the effects of the processing on the protection of personal data is available through the PDPS and at the address: GDPR Procedures**.**

15.5. Consultation with the supervisory authority

15.5.1. If the Company's assessment of the effects of the processing on the protection of personal data demonstrates that the processing of personal data would involve high risks if the Company did not take measures to minimise those

risks, the Company shall consult the supervisory authority before processing the personal data.

15.5.2. When consulting the supervisory authority, the Company shall provide the supervisory authority with:

(a) where applicable, the respective responsibilities of the Company, joint controllers and processors involved in the processing, in particular where personal data is processed within a group of companies;

(b) the purposes and means of the intended processing of the Personal Data;

(c) the measures and safeguards to protect the rights and freedoms of data subjects, in accordance with the GDPR;

(d) an assessment of the effects of the processing on the protection of personal data; and

(e) any other information requested by the supervisory authority.

15.5.3. The Company shall take into account the opinion of the supervisory authority and shall comply with any recommendations during and after the investigation.

15.6. Security measures

15.6.1. The Company shall apply security measures as determined by risk analyses and adequacy of security measures and assessments of the effects of the processing on data protection. The Company shall determine the organisational and technical measures of personal data protection that can be applied and assess the cost of their implementation. The Company shall adapt the protection measures to the level of risk.

(a) The organisational measures for the protection of personal data applied by the Company include in particular:

a. this Policy and other policies and procedures referred to in the Policy;

b. IT Security Policy, which is in force in the Company, its content is available in the IT Department and at the address: GDPR Procedures;

c. authorisations to process personal data;

d. rules of access control to premises and systems where personal data is processed;

e. up-to-date records of IT systems (and IT equipment used for processing information), including their type and configuration and assigning responsibilities to business owners of IT systems;

f. registers of processing activities and register of categories of processing activities;

g. the procedure for handling the register of breaches (included in the Procedure for assessment and notification of personal data protection breaches);

h. procedure for identification and evaluation of processors and an agreement (and appropriate templates) of entrustment of personal data processing concluded with processors;

i. a 'clean' desk policy, the content of which, applicable in the Company, is available through the PDPS and at the address: GDPR Procedures

j. a policy on the use of computers and mobile devices, which is available through the PDPS and at the address: GDPR Procedures

k. a policy governing the authorised use of personal devices for business purposes, as set out in the Company's policy, which is available through the PDPS and at the address: GDPR Procedures

l. a policy governing the use of removable IT media, the content of which is available through the PDPS and at the address: GDPR Procedures

m. conducting periodic analyses of the risk of loss of integrity, availability or confidentiality of information and taking actions to minimise this risk, according to the results of the conducted analysis;

n. including provisions in agreements with third parties guaranteeing an adequate level of security, in particular confidentiality obligations;

o. ensuring periodic internal information security audits at least once a year.

(b) Technical measures for the protection of personal data shall include in particular:

a. physical security measures on the premises and used on the premises where personal data is processed;

b. measures to prevent the consequences of breaches or disasters and to ensure business continuity – alarms, fire protection, physical protection, backup systems, archiving in closed rooms, etc;

c. measures to protect information systems, including anti-virus software, firewalls and network segmentation, system access control mechanisms based on unique identification of users or devices, event logging mechanisms, central management system for computers and mobile devices;

d. pseudonymisation;

e. encryption, in particular using the following solutions: S/MIME;

f. monitoring access to information through authorisations and access to information systems,

g. taking action to detect unauthorised processing activities,

h. *providing measures to prevent unauthorised access at the level of operating systems, network services and applications, in particular through access control mechanisms.*

i. *ensuring* an adequate level of security in information systems, consisting in particular of:

   i. ensuring that software is kept up to date,

   ii. minimising the risk of losing information as a result of failure,

   iii. protection against errors, loss, unauthorized modification,

   iv. use of cryptographic mechanisms in a manner adequate to threats or legal requirements,

   v. ensuring security of system files,

   vi. reducing risks resulting from the use of published technical vulnerabilities of ICT systems,

   vii. taking immediate actions after noticing undisclosed vulnerabilities of ICT systems to the possibility of a security breach,

   viii. checking the compliance of ICT systems with relevant security standards and policies.

15.6.2. Depending on the type of risk related to the given activity of personal data processing, the Company shall also apply other technical and organisational measures for personal data protection than those described in the foregoing points.

16. NOTIFICATION OF PERSONAL DATA PROTECTION BREACHES

16.1. The Company shall apply procedures to identify, assess and notify an identified case of personal data protection breach to the President of the Office for Personal Data Protection within 72 hours from the identification of the breach and, where required, to notify without undue delay data subjects of such a breach. The procedure for notification of personal data protection breaches constitutes Appendix No 4 to this Policy.

16.2. The Company shall maintain a Register of Personal Data Protection Breaches to document all cases of data protection breaches or suspected breaches. A template of the register of personal data protection breaches is attached as Appendix No 9 to this Policy.

16.3. In the event of a suspected or confirmed personal data breach, the Company shall keep the information in the register up-to-date throughout the investigation of the breach, including a preliminary risk assessment of the personal data breach. When performing the risk analysis, the Company shall take into account the circumstances listed in the register, as well as any other circumstances that may affect the degree of risk to the rights and freedoms of data subjects.

16.4. In the event of a personal data protection breach, the Company shall:

16.4.1. without undue delay but no later than within 72 hours of becoming aware of the breach, notify it to the competent supervisory authority, unless the breach is unlikely to result in a risk to the rights or freedoms of data subjects. A notification submitted to the supervisory authority after the expiry of 72 hours shall be accompanied by an explanation of the reasons for the delay; the template of the notification of a personal data breach to the supervisory authority is attached as Appendix No 5 to this Policy;

16.4.2. without undue delay, notify the data subject of such a breach, if the personal data breach is likely to result in a high risk of violation of the rights or freedoms of the data subject; a template of the notification of a personal data breach to the data subject constitutes Appendix No 6 to this Policy. Notification to the data subject is not required if:

(a) The Company has implemented appropriate technical and organisational protection measures and these measures have been applied to the personal data affected by the breach, in particular measures such as

encryption to prevent reading by unauthorised persons accessing such personal data;

(b) the Company has subsequently applied measures to eliminate the likelihood of a high risk of infringement of the rights or freedoms of the data subject;

(c) it would require a disproportionate effort. In such a case, a public notice shall be issued or a similar measure shall be taken by which the data subjects shall be informed in an equally effective manner.

16.5. Where a data protection breach relates to the processing of personal data by a Processor, such Processor shall (pursuant to the relevant contractual obligations) be obliged to notify the Company and co-operate with the Company in carrying out a risk analysis relating to the breach.

17. ENTRUSTING DATA PROCESSING

17.1. Entrusting the processing of personal data to a Processor by the Company

17.1.1. The Company, as part of the implementation of this Policy, permits personal data of which it is the controller to be processed outside its own organisational structures and in this regard the Company shall identify cases where it is necessary to entrust the processing of personal data to another entity.

17.1.2. The Company has developed and implemented procedures for the verification, evaluation and selection of processors to ensure that they provide sufficient guarantees to implement appropriate organisational and technical measures to ensure the security of personal data, the exercise of data subjects' rights and other personal data protection obligations incumbent on the Company. The Company verifies processors for providing sufficient guarantees in particular by:

(a) verifying how long the entity has been operating in the market;

(b) verifying the technical and organisational data protection measures adopted by the processor before entering into an agreement with the processor;

(c) appropriate statements contained in the agreement with the entity concerned;

(d) carrying out an audit of personal data processing at the processor´s premises.

17.1.3. The Company shall keep a register of processors, in which every entrusting of personal data processing is recorded. The person responsible for the execution of the subject of the agreement shall be responsible for informing the PDPS about the planned commencement of cooperation with the processor resulting in the need to conclude the entrustment agreement.

17.1.4. The processor identification procedure adopted by the Company and in force is available through the PDPS and at the address: GDPR Procedures

17.1.5. The processor evaluation procedure adopted by the Company and in force is available GDPR Procedures

17.1.6. The Company's adopted and applicable minimum technical and organisational requirements for processors are available through the PDPS and at the address: GDPR Procedures

17.1.7. Templates of personal data processing entrustment agreements are available through the PDPS and at the address: GDPR Procedures

17.2. Entrusting the processing of personal data to a Company (Company as a processor)

17.2.1. The Company identifies cases where it acts as a processor on behalf of another controller. The Company shall take care to conclude an appropriate agreement with the controller also on its own initiative in each case where it identifies a case of acting as processor.

17.2.2. The Company shall maintain and update a register of all categories of processing activities carried out on behalf of other controllers.

18. TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY

18.1. The Company shall, in connection with the entrustment of processing to a processor, the sharing of personal data with other controllers or the transfer of personal data to an international organisation, (i) verify whether the Company in such cases will transfer/ transfers data to third countries (as confirmed in the relevant entrustment agreements) and (ii) ensure that the legal basis for such a transfer is identified.

18.2. The transfer of personal data which is or is to be processed after such a transfer shall only take place if the Company and the data recipient (processor or other controller) comply with the additional requirements set out in the GDPR. In case the transfer of personal data to a third country or international organisation is necessary, the Company shall notify the data subject. A template of the data subject notification is attached as Appendix No 17 to this Policy.

18.3. The transfer of personal data to a third country or international organisation may be based in particular on:

18.3.1. a decision of the European Commission declaring an adequate level of protection in a third country or international organisation;

18.3.2. if no decision of the European Commission referred to in point 18.3.1 has been issued, the transfer is possible if appropriate safeguards referred to in Articles 46-47 of the GDPR have been applied, in particular:

(a) binding corporate rules adopted in accordance with Article 47 of the GDPR;

(b) standard data protection clauses adopted by the European Commission;

(c) standard personal data protection clauses adopted by a supervisory authority and approved by the European Commission;

(d) a code of conduct approved by the supervisory authority;

(e) certification in the field of personal data by a competent certification body;

(f) contractual clauses between the Company and the recipient of personal data (approved in advance by the supervisory authority).

18.4. The Company shall register the transfers of Personal Data to a third country and update the entries in the register.

19. FINAL PROVISIONS

19.1. The Company shall review the provisions of this Policy and any other procedures and policies referred to in this Policy at least once a year and update its provisions as necessary.

DETAILED PART

List of Appendices

1. A template of an authorisation to process personal data;
2. A template of the register of authorisations to process personal data
3. List of locations where personal data is processed;
4. Procedure for assessment and reporting of personal data protection breaches;
5. A template of the notification of a personal data breach to the supervisory authority;
6. A template of notification of a personal data breach to the data subject;
7. A template of the register of personal data processing activities;
8. A template of the register of all categories of personal data processing activities performed by the Company on behalf of another controller;
9. A template of the register of personal data protection breaches;
10. A template of the data subject's notification of data recipients pursuant to Article 19 of the GDPR;
11. A template of the information on the data subject's non-identifiability;
12. A template for responses to data subjects' requests;
13. A template for information on the reasons for not acting on the data subject's requests;
14. A template for the data subject's notice of extension of the time limit for processing the request;
15. A template of the notification to the data subject on lifting a restriction on processing of personal data;
16. A template of notification to recipients of the rectification / erasure / restriction of the processing of personal data
17. A template of the data subject notification on transfer of personal data to a third country;