Personal Data Controller

INTOBELLO SPÓŁKA
Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
UL. GRZYBOWSKA 87
00-844 WARSZAWA
KRS: 809144

Personal data protection policy of 24.10.2020 .

Having regard to the obligations arising from Articles 25 and 32 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.04.2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ EU L 119, p. 1), to ensure that personal data in Intobello sp. z o.o. based in Warsaw are processed and secured in accordance with the provisions of the law by implementing appropriate technical and organisational measures designed to effectively implement data protection principles, and to give the processing the necessary safeguards; and Intobello sp. z o.o. based in Warsaw ensures that, by default, only those personal data which are necessary for each specific purpose of processing are processed.

§ 1

Preliminary provisions

1.1, The Policy defines the principles of personal data processing and protection in the enterprise in order to ensure the convergence of the Processing with the requirements of the GDPR and the provisions of the mandatory Polish law on personal data processing. The Policy constitutes a set and basis for the requirements, procedures and principles of personal data protection implemented in the enterprise. The Policy includes:

- contains a description of the data protection rules applicable in the enterprise;
- a set of procedures, instructions and detailed regulations concerning personal data processing in the enterprise, concerning particular areas of personal data protection; constituting annexes to the Policy.

1.2, The Policy applies to all employees and associates of the company. The following entities are responsible for compliance and maintenance of the Policy:

- Controller:
- organizational units of the company where Personal Data are processed;
- Employees.

1.3. For the effective implementation of the Policy, taking into account the scope, context and objectives of the processing and the risk of infringement of the rights or freedoms of natural persons of varying probability and seriousness of the threat, the Controller ensures:

- implementation of appropriate technical and organizational measures to ensure compliance of the processing of Personal Data with the legal requirements and the necessary security of the processed personal data;
- constant monitoring of the compliance of the processing of Personal Data with legal requirements and subjecting the measures referred to in paragraph 1.3. to constant review and updating;

- control and supervision over the processing of Personal Data.

1.4. The supervision of compliance with the policy provisions shall be ensured by the Data Controller. The supervision referred to in the preceding sentence aims, in particular, but not exclusively, at ensuring that the activities related to the processing of Personal Data in the company are in accordance with the requirements of law and the provisions of the Policy.

1.5. The Controller shall ensure that the conduct of the contracting parties, including in particular the Processing Entities, complies with the provisions of the Policy to an appropriate extent in all situations where the Personal Data is transferred to these entities for processing, including storage.

1.6. The Policy shall be stored and made available in a paper and electronic version at the Company's seat.

1.7. The Policy is made available:

- obligatorily to all persons authorized to process Personal Data in the enterprise, in order to provide authorized persons with proper knowledge and information on the principles and requirements for processing Personal Data in the enterprise;
- to the persons concerned, in particular to the natural persons being data subjects - at their request.

§ 2

Glossary

2.1. Whenever the following definitions or phrases are used in this Policy, they shall have the following meaning:

- Policy - means this Policy and all its possible Attachments;
- Personal Data - means information about an identified or identifiable natural person, such as name, identification number, location data, internet identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of an individual; as referred to in Article 4(1) of the GDPR;
- GDRP - the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/04/2016 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 regulation on data protection) (OJ, UE L 119, p. 1);
- Authorized person - means a person authorized by the Controller to process Personal Data in a given scope;
- Processing - shall mean any operation or set of operations which is performed on personal data or sets of personal data by automatic or non-automated means, such as collection, recording, organisation, structuring, storage, adaptation or modification, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion or destruction referred to in Article 4 (2) of the GDPR;
- Filing system - means any structured set of Personal Data which is accessible according to specific criteria;
- Processor - means any natural or legal person, public authority, entity or other body which processes personal data on behalf of the Controller;
- Authentication - means an action whose purpose is to verify the declared identity of the User;
- Controller – means Intobello spółka z ograniczoną odpowiedzialnością, ul. Grzybowska

87, 00- 844 Warszawa entered in the Register of Entrepreneurs of the National Court Register kept by the District Court for the Capital City of Warsaw, in Warsaw, XII Commercial Division of the National Court Register under the number: 809144, NIP *[Taxpayer ID No.]*: 52272909135, REGON [Business Entity no.]: 384672288

- Employees - means both persons employed in the company on the basis of an employment relationship and natural persons cooperating with the company on the basis of a civil law contract;
- System - means the Personal Data Protection System in the enterprise referred to in § 5 of the Policy;
- Sensitive Data - means the Personal Data referred to in Article 9 of the GDPR.

§ 3

Personal data

3.1. The Controller processes the Personal Data collected in the filing systems. The filing systems processed in the enterprise are specified in Attachment 1 to the Policy.

3.2. The list of filing systems shall be updated or extended after prior analysis of the effects and risks of personal data processing on the rights and freedoms of natural persons covered by the filing system.

3.3. The Controller shall not undertake any Processing activities which could involve a significant risk of infringing the rights and freedoms of the individuals covered by the Personal Data. In case of planning to undertake activities referred to in the preceding sentence, the Controller shall obligatorily carry out a prior evaluation of the effects of the processing referred to in Article 35 of the GDPR.

3.4. By default, Personal Data shall be processed in the area including the enterprise's office premises located in Warsaw at ul. Grzybowska 87. An additional area where Personal Data is processed is all portable computers and other data carriers located outside the area indicated in the preceding sentence.

§ 4

Basics of Personal Data Protection

4.1. The Controller shall ensure that the technical and organisational measures necessary to ensure confidentiality, integrity, accountability and continuity of the data processed are applied.

4.2. Authorized persons and all other persons to whom the Personal Data Processed in the enterprise are made available shall be obliged to Process the Personal Data in accordance with legal requirements and in accordance with the provisions of the Policy, as well as other internal legal acts of the Controller or internal procedures related to the Processing of Personal Data.

4.3. When hiring Employees and in the course of their employment, the Controller ensures that:

- Employees shall receive appropriate knowledge of the principles of Processing and Protection of Personal Data before commencing their duties;
- each Employee is authorised in writing to Process Personal Data to the extent necessary, in accordance with the template constituting Attachments 2 to the Policy;
- each of the Employees is obliged to maintain the confidentiality and integrity of Personal Data in accordance with the template constituting Attachment 3 to the Policy, whereby the Employees are obliged in particular, but not exclusively, to:

- ✔ strictly observe the scope of authorization;
- ✔ comply with legal requirements and the provisions of the Policy with regard to processing;
- ✔ keep the Personal Data confidential;
- ✔ keep the confidentiality and integrity of Personal Data confidential;
- ✔ immediately report to the Controller any incidents related to the breach of security of Personal Data.

4.4. The Controller ensures that the Personal Data are:

- Processed lawfully, fairly and transparently to the data subject;
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- adequate, relevant and limited to what is necessary for the purposes for which they are processed;
- adequate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which are inaccurate in relation to the purposes for which they are processed are immediately deleted or rectified ('accuracy');
- kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data are processed;
- processed in such a way as to ensure adequate security of personal data, including protection against illegitimate or unlawful processing and accidental loss, destruction or damage, by appropriate technical or organisational measures.

4.5. When ensuring the Processing of Personal Data in accordance with the principles indicated in section 4.1 above, the Controller shall base the Processing on the following grounds:

- Legitimacy - the Controller cares for the protection of privacy and processes the Personal Data in accordance with legal requirements;
- Security - the Controller ensures an appropriate level of security of the Personal Data by taking permanent actions in this respect;
- Rights of the Individual - the Controller enables the persons whose Personal Data is being processed to exercise their rights and exercises these rights;
- Accountability - the Controller shall ensure that the manner of fulfilling the obligations in the scope of personal data protection is duly documented.

.

§ 5

Personal data protection system

5.1. The Controller ensures compliance of the Personal Data Processing with legal requirements also by designing, implementing and maintaining the System The System consists of organizational and technical measures of protection, adequate to the level of risk identified for individual filling systems and data categories. The System consists in particular of the following measures:

- limiting access to the premises where Personal Data are processed only to Authorized Persons and ensuring that other persons may stay in the premises used for the Processing of Personal Data only in the company of an Authorized Person;
- closing the premises forming the area referred to in section 3.4 of the Policy for the time of the absence of the Employees, in a manner preventing access to them by third

parties;

- ensuring protection of the area referred to in section 3.4 of the Policy against random factors such as fire or flooding;
- use of lockable cabinets, drawers or other technical means to prevent unauthorised access to the Personal Data stored therein;
- implementation of the Clean Desk Policy, which constitutes Attachment 4 to the Policy;
- ensuring effective removal or destruction of documents containing Personal Data in a way that makes their subsequent reproduction impossible;
- ensuring hardware and IT security, including
  - ✔ protecting the local network against activities initiated from outside,
  - ✔ ensuring that the software used is up-to-date,
  - ✔ protecting computer equipment used in the enterprise against malicious software,
  - ✔ ensuring constant and frequent back-up of data stored on computers, servers and the Controller's network,
  - ✔ Restrict access to computer hardware, server and local network by applying Authentication rules;
- carrying out risk analysis for data processing activities or categories of data;
- implementation of standards for verification and selection of Processors, as well as conditions for entrusting Data Processing to individual Processors;
- monitoring of changes in the scope of Personal Data Processing processes in the enterprise and managing changes affecting the protection of Personal Data in the enterprise on an ongoing basis.

§ 6

Fulfilment of obligations towards the data subjects

7.1. The Controller shall implement methods for managing consents that enable the registration and verification of a person's consent to the processing of his/her specific data for a specific purpose, consent to remote communication (e-mail, telephone, SMS, etc.) and the registration of refusal of consent, withdrawal of consent and similar activities such as objection or restriction of processing.

7.2. The Controller takes care of the legibility and style of information and communication with persons whose Personal Data he processes.

7.3. The Controller shall publish on the website and leave as follows for inspection at the Company's registered office:

- Policy;
- Information on data subjects' rights;
- Information about the scope of personal data processed for specific purposes;
- Methods of contact with the Controller with regard to personal data;

7.4. For the purpose of exercising the rights of the Data Subject, the Controller shall provide procedures and mechanisms to identify the data of specific persons processed by the Controller, integrate the data, introduce changes and delete them in an integrated manner.

7.5. The Controller shall document the handling of information obligations, notices and requests

of persons by informing the data subject:

- about the processing of his data, when collecting data from that person
- about the processing of his or her data, when acquiring data about that person not directly from him or her;
- about the planned change in the purpose of the data processing.
- before cancellation of the processing restriction.
- about the rectification, erasure or restriction of processing (unless this will involve disproportionate effort or is impossible).
- about the right to object to the processing of the data at the latest on the first contact with that person.

7.6. The Controller shall, without undue delay, notify a person of a personal data protection breach, if it may cause a high risk of violating that person's rights or freedoms.

7.7. Irrespective of the provisions of paragraph 7.5 above, the Controller shall determine the manner of informing persons about the processing of unidentified data, where possible (e.g. a plate with information about being subject to video surveillance).

7.8. At the request of a person concerning access to his/her data, the controller shall inform the person whether he/she is processing his/her data and shall inform the person about the details of the processing, according to Article 15 of the GDPR, as well as give the person access to the data concerning him/her. The access to the data may be realized by issuing a copy of the data.

7.9. The Controller issues a copy of the data to a person being the data subject and records the fact of issuing the first data copy.

7.10. The Controller shall correct incorrect data at the request of the Data Subject. The controller has the right to refuse to rectify the data, unless the person reasonably proves the incorrectness of the data which he or she requests to be corrected. In the case of the rectification of data, the controller shall inform the person about the recipients of the data, at that person's request.

7.11. The controller shall complete and update the data at the request of the data subject. The controller has the right to refuse to complete the data if the completion would be incompatible with the purposes of data processing. The Controller may rely on the person's declaration as to the data to be completed, unless it is insufficient in the light of the procedures adopted by the Controller, the law or there are grounds to consider the declaration unreliable.

7.12. Subject to paragraph 7.13 below, at the request of a person, the Controller shall delete the data when:

- the data are not necessary for the purposes for which they were collected or processed for other purposes,
- consent to their processing has been withdrawn, and there is no other legal basis for the processing,
- the person has raised an effective objection to the processing of these data,
- the data were processed illegally,
- the need for removal results from a legal obligation,
- the request concerns data of a child collected on the basis of consent in order to provide information society services offered directly to the child.

7.13. When deleting personal data, the Controller shall take into account to ensure the effective exercise of this right with respect to all the principles of data protection, including security,

as well as to verify whether the exceptions referred to in Article 17(3) of the GDPR, does not occur

7.14. If the data to be deleted have been made public by the Controller, the Controller shall take reasonable actions, including technical measures, to inform other controllers processing these personal data about the need to delete the data and access to them. In case of data deletion, the Controller shall inform a person about the recipients of the data, at that person's request.

7.15. The controller shall restrict the processing of the data at the request of the person when:

- the person contests the correctness of the data - for the period allowing to check their correctness,
- the processing is unlawful and the data subject opposes the deletion of the personal data, demanding instead a restriction on its use,
- The Controller no longer needs personal data, but it is needed by the data subject to establish, pursue or defend a claim,
- a person has lodged an objection to the processing on grounds related to his or her particular situation - until it is determined whether there are legally valid grounds for objection on the part of the Controller.

7.16. In the course of restricting the processing, the Controller shall store the data, but shall not process them (not use, not transfer), without the consent of the data subject, unless for the purpose of determining, asserting or defending claims, or to protect the rights of another natural or legal person, or for important reasons of public interest. The Controller shall inform the person before annulment of the processing restriction. In case of a restriction of data processing, the Controller shall inform the person about the recipients of the data, at the request of this person.

7.17. At the request of a person, the Controller shall issue in a structured, commonly used machine-readable format or transfer to another entity, if possible, data concerning that person which the person has provided to the Controller , processed on the basis of that person's consent or for the purpose of concluding or performing an agreement concluded with him/her, in the Controller 's IT systems.

7.18. If a person objects to the processing of his/her data, referred to in Article 21 of the GDPR, justified by his/her particular situation, and the data are processed by the Controller on the basis of a legitimate interest of the enterprise or a task entrusted to the Controller in the public interest, the Controller undertakes to take into account the objection, unless there are valid legal grounds for processing on the part of the Controller overriding the interests, rights and freedoms of the objector or grounds for establishing, pursuing or defending claims.

7.19. If a person objects to the processing of his/her data by the Controller for the purposes of direct marketing, the Controller will take into account the objection and discontinue such processing.

§ 8

Data Minimization

8.1. The Controller shall implement procedures for the implementation of the principle of minimizing the personal data processed in terms of

- adequacy of Personal Data for the purposes of processing, including limitation of the amount of Personal Data being processed and the scope of processing to the purpose of processing;
- restriction of access to the Personal Data only to Authorized Persons for whom the use of

the Personal Data in a specific scope is necessary for the proper performance of their duties

- limit the time of storage of Personal Data to the period for which storage of Personal Data is necessary due to the realization of the purpose of Processing or obligations imposed on the Controller.

8.2. The Controller shall periodically review the amount and scope of Processing at least once a year.

8.3. The Controller shall apply restrictions of access to the Personal Data through implementation:

- obligation of Employees to keep the Personal Data confidential;
- verifying the circle of internal recipients of the Personal Data by granting individual Employees specific authorization to Process the Personal Data;
- implementing logical technical measures to protect Personal Data by limiting access to systems, software, and network resources used for the processing of Personal Data;
- implementing technical measures to protect Personal Data as described in section 5.1. of the Policy.

8.4. The Controller shall update access rights in the event of changes in the composition of personnel and changes in the roles of persons, and changes in the processing entities. The Controller shall periodically review the established system users and update them at least once a year.

8.5. Detailed rules of physical and logical access control are included in the physical and information security procedures.

8.6. Data which usefulness is limited over time shall be removed from the systems as well as from the reference and master files. Such data may be archived and placed on backup copies of systems and information processed by the Controller. The procedures for archiving, creating and using backups shall take into account the requirements of data lifecycle control, including data deletion.

§ 8

Personal data protection

9.1. Taking into account the state of technical knowledge, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risk of infringement of the rights or freedoms of natural persons with different probability and seriousness of the threat, the Controller shall implement technical and organizational measures ensuring an adequate level of protection of Personal Data, corresponding to the risk of infringement of the rights and freedoms of natural persons as a result of personal data processing by the Controller .

9.2. The Controller shall perform and document analyses of adequacy of personal data security measures. For this purpose:

- categorise the data and processing activities in terms of the risks they present;
- conduct analyses of the risk of infringement of rights or freedoms of natural persons for data processing activities or their categories. The Controller shall analyse possible situations and scenarios of personal data protection violation taking into account the nature, scope, context and purposes of the processing, the risk of violation of rights or freedoms of natural persons with different probability of occurrence and severity of the threat;

9.3. The Controller implements measures to ensure business continuity and disaster prevention,

i.e. the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident.

§ 10

Breach of personal data protection

10.1. As a breach or attempted breach of the principles of processing and protection of Personal Data shall be considered in particular, but without limitation to:

- breach of security of information systems in which personal data are processed;
- making personal data available to unauthorised persons;
- processing of personal data contrary to the assumed scope and purpose of their processing;
- unauthorized or accidental damage, loss, destruction or change of Personal Data.

10.2. In the event of finding a personal data protection breach, the Controller shall assess whether the breach may have caused a risk of infringing the rights or freedoms of natural persons and assess the scale of the risk.

10.3. In case of a personal data protection breach, the Controller shall, without undue delay - as far as possible, not later than 72 hours after the discovery of the breach - report it to the competent supervisory authority, unless the breach is unlikely to result in a risk of violation of the rights or freedoms of natural persons. A notification template, referred to in the preceding sentence, is attached as Attachment 5 to the Policy.

10.4. If the risk of infringement of the rights and freedoms of the Data Subject is high, the Controller shall also notify the incident to the Data Subject, unless:

- The Controller shall implement appropriate technical and organisational protection measures and these measures have been applied to the personal data to which the incident relates, preventing the reading of such data by unauthorised persons;
- The Controller shall then apply measures to eliminate the likelihood of a high risk of infringement of the data subject's rights or freedoms;
- This would require a disproportionate effort. In such a case, a public communication shall be issued or a similar measure shall be taken by which data subjects shall be informed in an equally effective manner.

10.5. Notwithstanding the obligations set forth in sections 10.2-10.4 above, the Controller shall document any personal data breach, including the circumstances of the personal data breach, its effects and remedial actions taken. A template of the register of personal data breaches is attached as Attachment 7 to the Policy.

§ 11

Entrustment of processing

11.1. The Controller may entrust the Processing of Personal Data to the Processor only by means of an agreement concluded in writing, according to the requirements indicated in Article 28(3) of the GDPR.

11.2. The Controller shall only use the services of such Processors which provide sufficient guarantees for the implementation of appropriate technical and organisational measures to ensure that the processing meets the requirements of this Regulation and protects the rights of the data subjects. In order to verify the fulfilment of the obligation referred to in the preceding sentence, before entrusting the processing to a potential Processor, the Controller shall, as far as possible, obtain information about the personal data protection rules applied

by the potential Processor, and about the personal data protection practices of the potential Processor.

§ 12

Transfer of data to a third country

12.1. The controller shall not transfer Personal Data to a third country outside the European Union or the European Economic Area, except at the request of the Data Subject.

12.2. In order to avoid situations of unauthorized data export, in particular in connection with the use of publicly available cloud services, the Controller periodically verifies users' behaviour and, as far as possible, provides equivalent solutions in accordance with data protection law.

§ 13

Final Provisions

13.1. The Data Protection Policy is an internal document and must not be made available to unauthorised persons in any form.

13.2. Each person processing personal data shall read the contents of the Personal Data Protection Policy and undertake to strictly apply the provisions contained therein when processing personal data.

13.3. The policy shall enter into force on the date of its announcement.

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

13.5. Any amendments or supplements to the Policy shall be made in writing to be effective, otherwise they shall be null and void. The amendments or supplements to the Policy shall come into force not earlier than within 7 days of their announcement.

13.6. The following Appendices, constituting an integral part of the Policy, have been attached to the Policy:

- Attachment No. 1 - List of filing systems;
- Attachment No. 2 - Template of authorisation to process personal data;.
- Attachment No. 3 - Template of commitment to confidentiality;
- Attachment No. 4 - Clean Desk Policy;
- Attachment No. 5 - Register of processing activities;
- Attachment No. 6 - Template of personal data protection breach notification;
- Attachment No. 7 - Register of personal data breaches;

Attachment No. 1 - List of filing systems

No.	NAME OF THE FILING SYSTEM	SUB-SYSTEMS	FILING SYSTEM STRUCTURE
1	**EMPLOYEES AND PERSONS PROVIDING SERVICES BASED ON CIVIL LAW CONTRACTS**	-personal data of employees, -payrolls, -records of the employees, -time record, -business trips, -worker accidents, -bailiff activities -personal details of contractors and performers, -insurance documentation	-name and surname, -PESEL registration number, -sex -parents' names -citizenship -personal identity card (series, number, by whom issued, date of issue) -date and place of birth -registration address - mailing address - telephone number - family status -treasury office - pension no. - employment history -training (name of school, year of graduation)
2	**CONTRACTOR FILING SYSTEM**	-invoices, -bills, -contracts, -other sales/purchase documents.	-name and surname, -PESEL registration number, -address of residence or stay, -personal identity card (series, number, by whom issued, date of issue), -nos. of bank accounts of contractors who are natural persons, -NIP.
4	**FILING SYSTEM IN THE FORM OF ACCOUNTING DOCUMENTS**	-journal -books, -financial reports, -CSO reports, - tax declaration, -Vat registers, -additional accounting records.	-name and surname, -PESEL registration number, - address of residence or stay, -personal identity card (series, number, by whom issued, date of issue), -nos. of bank accounts of contractors who are natural persons, -NIP.
6	**VIDEO SURVEILLANCE**	-monitoring record	- image.
7	**REGISTER OF CORRESPONDENCE**	-register of incoming correspondence, - register of outgoing correspondence.	-recipient's name and surname, -date of receipt: -address for delivery.

Attachment no. 2 - Template of authorisation to process personal data

. . . .date. . . . . .
[place, date of preparation]

AUTHORISATION TO PROCESS
PERSONAL DATA

Acting on behalf of ... . I hereby authorize:

Ms/Mr . . . . . .

Position ....

for the processing of personal data in connection with the provision of services to ... .
. . . . . .

in the following scope: .....

A. Period of authorisation:

1. For the period of employment/cooperation in accordance with the contract of employment;
2. Contract status: active.

B. Scope of authorisation:

1. Data processed on paper,
2. Information system,
3. Personal data covered by the filing system:

a). . . . . .

b) . . . . . .

c) . . . . . .

* without limitation, data view, data entering, data processing,
data change, data deletion, on mobile computers)

. . . . . .
[Data Controller]

Attachment No. 3 - Template of commitment to confidentiality

. . . . . (date) . . . . . .

[place, date of preparation]

. . . . . .
name and surname of the authorized person:
. . . . . .
position:
. . . . . .
place of work;

REPRESENTATION

I represent that in connection with my work for ..... and authorising me to process Personal Data, I have been acquainted with the relevant regulations and standards of personal data protection, and I undertake to comply with them:

1. Rules on personal data protection, including the Regulation of the European Parliament and the Council (EU) 2016/679 of 27 April 2016 on the protection of natural persons in connection with the processing of personal data and on the free movement of such data and the repeal of Directive 95/46/EC
2. Information Security Policy in . . . . . .

Therefore, I undertake to:

1. ensure protection of personal data processed in the controller's files, and, in particular, to ensure their safety to not be made available to third parties and unauthorised persons, taking away, damaging and unjustified modification or destruction,
2. maintain secrecy, even after the work has ceased, of any information on the functioning of the systems used for processing of personal data
3. immediately report to the Data Controller the observed attempt or actual breach of physical security of the room, security of file/files or information systems.

. . . . . .

[employee/cooperator signature]

Attachment No. 4 - Clean Desk Policy

Clean Desk Policy

1. The policy regulates the requirements and procedures for the protection of confidential data, including personal data processed in ..... by Employees in paper form, including
    a. paper documents;
    b. mail correspondence;
    d. source documents
    e. official correspondence.
2. Whenever the following definitions and phrases are used in the Policy, they shall have the following meaning:
    a. Policy - means this Clean Desk Policy and all possible attachments;
    b. Employee - means both any natural person employed on the basis of an employment contract, as well as cooperating on the basis of a civil law contract (including in the scope of sole proprietorship) and a student or pupil who is not an employee during an internship or work placement;
3. The policy applies to all Employees, regardless of their position and time of employment.
4. Each Employee shall be obliged to limit the access of outsiders to confidential data, including personal data contained on paper media used by the Employee in the performance of his/her duties.
5. In the course of work, each Employee is obliged to keep on his or her desk or at his or her workplace only those documents which are necessary for the performance of current tasks at a given moment of work. If the given documents are no longer necessary for the Employee to perform current tasks, the Employee is obliged to put them away. The provisions of paragraph 6 below shall apply accordingly.
6. If an employee leaves his or her desk or workplace, even temporarily, the employee is obliged to put and hide all used documents containing confidential or personal data in a lockable drawer or cupboard in order to prevent access to documents by outsiders.
7. If an Employee finishes work on a given day, the Employee is obliged before leaving the premises to perform the obligation referred to in section 6 above and to secure the documents against access by any third parties. After the completion of work, the desk may only contain a landline phone and office supplies.
8. The employee is obliged to ensure that in the course of work at the workplace there are no liquids or other substances threatening to destroy or damage paper documents when they are spilled. On the same basis, the employee shall refrain from eating at his desk or workstation.
9. Notwithstanding the provisions of sections 4-8 above, after finishing work, an Employee is obliged to put his company laptop in a lockable cabinet in order to prevent access to the data stored on the company computer by outsiders.
10. If a given document will not be used anymore, as well as in situations specified in the Personal Data Protection Policy, the Employee is obliged to ensure immediate destruction of unnecessary documents in such a way that it is not possible to reconstruct the information contained therein, unless the Personal Data Protection Policy provides for a different way of disposing of the documents or orders to leave or archive them.

.....

Controller

Attachment No. 5 - Template of personal data protection breach notification

. . . . . , date . . . . . .

[place, date of preparation]

President of the Office for Personal Data Protection

. . . . . .

REPORTING A PERSONAL DATA BREACH INCIDENT

Acting on the basis of Article 33 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), I hereby report an incident involving a breach of the personal data protection.

Data of the Personal Data Controller	
Place and day of breach	
Category and approximate number of data subjects	
Categories and approximate number of personal data entries affected by the breach	
Description of the nature of the data protection breach	
Possible consequences of a data protection breach	
Measures taken to minimise the possible adverse effects of the data protection breach	

. . . . . .

[signature of the person authorised to represent the Data Controller]

Attachment No. 6 - Register of personal data protection breaches

No	Description of the circumstances of the breach/incident	Number of persons affected by the breach/ incident	Effects of the breach/ incident	Remedial action	Breach/incident resulting in/risks to the rights or freedoms of individuals. Notification to the President of the Office for Personal Data Protection (YES/NO)	Date of completion of implementation of corrective measures	Person responsible for implementing the measures	Breach of the protection of personal data, resulting in a high risk of violation of the rights or freedoms of individuals. Notification of the incident to the data subject (YES/NO)
1								
2								
3								
4								
5								
6								
7								