Personal Data Protection Policy

Asseco Business Solutions SA

Version 1.0

Effective from 2 July 2018

Legal/statutory/corporate basis: Resolution of the Management Board of 2 July 2018

This document is for informational purposes only. The only official version is the Polish one as approved by the Management Board

1. Definitions

Defined below are the fundamental concepts used in the Personal Data Protection Policy (PDPP):

1.1. ABS SA–Asseco Business Solutions SA; data controller in the context of the PDPP, i.e. the entity that determines the purposes and means of the processing of personal under its care and custody.

1.2. Access rights management–decisions made by the domain-specific application owner on granting or denying access to the application as required by the business process supported by the given domain-specific application.

1.3. Access Rights Table (ART)–information on the level of access to personal data available via a given domain-specific application to each of the employees authorized to use it (see Section 4). The latest ART is kept in the RU resources.

1.4. Consent to processing–a voluntary, conscious and express declaration of will made by a data subject to have their data processed for a clearly defined purpose.

1.5. Data processing–any operations on data, e.g. storage, change of format, sharing, etc.

1.6. Data Protection Officer (DPO)–a person who supervises compliance with the personal data protection requirements as well as performing the tasks listed in Article 39 GDPR; the DPO is appointed by a resolution of the Management Board of ABS SA.

1.7. Data subject–according to the GDPR, an identified or identifiable natural person relating to data.

1.8. Data sharing–any activity by a person or a domain-specific application that can lead to any data being shared with, or provided to, a person or another domain-specific application obtaining data.

1.9. Domain-specific application owner (DSAO)–a person who determines:

(a) the purpose of maintaining the application, (b) the financial and organizational measures necessary to maintain the application, (c) the manner of using the application to achieve the purpose by other persons, including the managing of their access rights to the application.

1.10. Domain-specific application–a computer program or a traditional information processing tool used in the ABS SA business processes; for the purposes of the PDPP the extent of domain-specific applications is restricted only to those handling the processing of personal data.

The method of isolation of a given domain-specific application from the ABS SA resources and the method of its communication with other applications is determined by the domain-specific application owner and at their discretion:

- in liaison with each owner of any other domain-specific application which communicates directly with the given domain application;

and

- having regard to the relevant security policy for a media carrier (e.g. computer network, security cabinet with files, etc.) as provided in the NSP.

Examples of domain-specific applications:

- a computer program whose functions allow the user to handle and support their selected business-specific processes. Examples of domain-specific applications:
- software for HR and payroll management,
- software for book-keeping and generating financial reports,
- software for customer relationship management (CRM),
- a data stream provided via a specific communication protocol from a defined source (e.g. HTTP server, SOA data bus, etc.),

any non-automated methods of organizing information, such as:

- paper binders with indexes,
- removable external drives or other external mass storage solutions.

Due to the technical progress, it is impossible to enumerate all existing domain-specific applications.

1.11. Domain-specific application administrator (DSAA)–a person responsible for maintaining the technical performance of this application and for ensuring the protection of information made available via the application in a manner consistent with its operation manual.

The DSAA grants (or denies) access at the request of the domain-specific application owner or another person authorized by the owner.

1.12. DPIA (*Data Protection Impact Assessment*)–a responsibility of the data controller, referred to in Article 35 GDPR, to carry out an assessment of the impact of the envisaged processing operations on the rights and freedoms of data subjects and to analyze the impact of personal data processing on their protection.

1.13. Erasure of data–the processing of data as a result of which it is no longer possible to make any previously retained data available again.

1.14. Employee–a person employed by ABS SA under a contract of employment or cooperating with ABS SA under a service contract (dependent subcontractor).

1.15. GDPR–General Data Protection Regulation, i.e. 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).

1.16. Identification–the processing of certain data by any technical or organizational measures that are reasonably likely to be used (in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that identified data subject), leading to the effective identification of a specific data subject.

1.17. Network Security Policy (NSP)–a set of rules to be observed at ABS SA in order to ensure the proper protection of stored information and to make it available to its users on the hardware infrastructure using operating system and authentication services, identity confirmation services and directory-related services, and to manage network access, including via the Internet. The NSP is a separate document which, along with the GDPR, is part of the information security policy at ABS SA.

1.18. Personal data–all information relating to a data subject. It contains information that permit the identification of a data subject and information concerning that data subject directly.

The full text of the GDPR can be found at bit.ly/2DhOR6V.

1.19. RODO Utility by Asseco (RU)–an application supporting ABS SA in achieving compliance with the provisions of the GDPR, handling the logging of incidents and information related to the protection of personal data.

2. Introduction

2.1. Personal Data Protection Policy (PDPP)–a set of rules that must be followed by ABS SA in order to ensure the proper protection of personal data in line with the provisions of the GDPR.

2.2. The PDPP is based on the following assumptions:

- *access to information should be granted to everyone who needs it for the performance of their duties while protecting this information against unauthorized persons, at cost commensurate to the risk of threat to and the importance of protected information,*

- the basic form of protected information is electronic form, and access to this information is provided via a computer network,
- access to information stored in the ABS SA resources is contingent upon the access rights to these resources conferred on persons performing specific roles within the organization, such roles being assigned in accordance with the rules for the management and protection of computer network resources as provided in the NSP.

2.3. Where the GDPR provisions do not apply, the rules set out in the NSP do.

2.4. The PDPP and other documents related to the protection of personal data at ABS SA are published at assecobs.pl/RODO website.

2.5. Violation of the obligation to comply with the PDPP, including pursuant to generally applicable law, may be considered–depending on the violating entity:

- a serious violation of employee duties justifying the termination of the contract of employment as provided in Article 52§1(1) of the Labor Code,

or

- a major reason justifying immediate termination of the contract with a contractor.

2.6. Nothing in the PDPP can justify the evasion of the obligation to adhere to applicable law. It is the intention of ABS SA for the provisions of the PDPP to implement some of the universally applicable regulations where it is required by circumstances or interest of ABS SA while abiding by the law. If in doubt as to the application of the PPDD, please consult the DPO.

3. Privacy policy

3.1. ABS SA processes personal data only when it is lawful, as provided in Article 6(1) GDPR and Article 9(2)(b) GDPR, when it, or a data subject, fulfils the duties and exercises specific rights with regard to labor law, social security, and social protection.

3.2. Regardless of the above, it is forbidden to perform data processing activities going beyond the processing activities set in the record of processing activities, in accordance with its current status in RU.

3.3. A data subject has the right to access data, rectify it, obtain the erasure or restriction of its processing; they also have the right to object to the processing of their personal data and to their transfer. In order to enable the exercise of these rights, ABS SA provides the electronic mail address odo@assecobs.pl.

3.4. ABS SA will refuse to erase data if such data is necessary to lodge, assert or defend against a claim or to meet a legal obligation of processing under EU or Polish law.

3.5. ABS SA shares personal data on the basis of a legitimate interest or in performance of agreements of processing personal data or to entities authorized to access such data under the law or with by data subject's consent.

4. Protection of access to data by a domain-specific application

4.1. Each director of any ABS SA department has the right to establish a domain-specific application. Once established, the application is owned by the person establishing it (DSAO).

4.2. The DSAO appoints the administrator of an established domain-specific application. However, if the appointed person is not officially subordinate to the owner, their supervisor must consent to such appointment.

4.3. The DSAO supervises the administrator by assigning them the task of maintaining the application, regardless of their official subordination, until the administrator's appointment is terminated. The DSAO may, at any time, terminate the administrator's appointment at their own discretion.

4.4. The DSAO is at all times responsible for ensuring the protection of personal data processed with the application, including by appointing the relevant personnel and guided by the assumptions contained of Section 2.2.

4.5. The DSAO is obliged to notify the DPO of their intention to establish a new domain-specific application and to provide a complete description of the processing activities and the result of DPIA for, and to the extent related to, the processing of personal data using the application to handle relevant business processes. The DPO is required to respond to this notification within two weeks and name any requirements that must be met in order for the new application to be established.

4.6. The DSAO may disable the application only having made sure that there is no such personal data that can only be accessed via this application in a structured and commonly used machine-readable format.

4.7. Personnel processing personal data using traditional domain-specific applications–most often in paper form–are required to safeguard such data in a manner corresponding to the nature of operation of the relevant traditional domain-specific application. In particular, the

"clean desk" rule/policy should be followed, and documents should be locked in rooms, cabinets, drawers, or safes.

5. Authorization to process personal data

5.1. Each employee, when requested to process personal data (or so required under a service contract), is considered authorized to such processing provided that:

5.1.1. the processing is done via a domain-specific application which, at the time of processing, has the appropriate access rights set up for the processing employee,

5.1.2. they have submitted the Employee Declaration regarding the content of the PDPP and has undertaken to be bound by it. A sample declaration is provided in Section I.4.

5.2. Employee's (application operator's) access rights are defined in the Access Rights Table and allow for the following parameters:

5.2.1. employee's role in the business process or position occupied within the organizational structure,

5.2.2. operator's identifier linked to a domain-specific application,

5.2.3. the categories of data subjects and categories of personal data whose processing is permissible to a given domain-specific application operator.

5.3. The DSAO is responsible for the correct definition of the parameters of the Access Rights Table, ensuring that the personal data processing rules listed in Article 5 GDPR are followed.

5.4. The DSAA is responsible for the correct set-up of the parameters of the Access Rights Table at DSAO's request.

5.5. The DSAO informs the DPO immediately about any change to the content of the Access Rights Table for any given application.

6. DPIA

6.1. When the processing of personal data using a domain-specific application is very likely, due to its nature, scope, context and purposes, to create a high risk of violating the rights or freedoms of data subjects, the DSAO assesses the impact of personal data processing on the rights and freedoms of data subjects (DPIA) before starting the processing.

6.2. The DPIA is carried out based on the guidelines of ISO 29134.

6.3. In order to carry out the DPIA, the DSAO may, and has the right to, hold a consultation with the DPO.

7. The processing of data obtained from a data subject

7.1. ABS SA processes personal data of a data subject obtained from that data subject when:

7.1.1. the data subject has given consent to the processing (Article 6(1)(a) or Article 9(2)(b) GDPR),

7.1.2. processing is necessary for compliance by ABS SA with a legal obligation (Article 6(1)(c) GDPR),

7.1.3. processing is necessary for the purposes of the legitimate interests pursued by ABS SA (Article 6(1)(f) GDPR),

7.1.4. processing is necessary for the conclusion and performance of a contract with a natural person or economic operator (Article 6(1)(b) GDPR).

7.2. In the case of processing personal data based on the data subject's consent, ABS SA follows the guidelines of the processing consent contained in Appendix D.

7.3. When obtaining personal data, ABS SA informs the data subject of their special rights under Article 13 GDPR (information clause). The detailed scope of such information and the sample clauses are contained in Appendix E.

7.4. ABS SA immediately responds to submitted legitimate data subject's requests following the information provided to them as referred to in Section 7.3.

8. The processing of data obtained from another controller

8.1. ABS SA processes personal data of a data subject obtained from another controller when:

8.1.1. it concludes a contract with another controller, and such a contract each time requires that controller to ensure the lawfulness of the processing of personal data

8.1.2. processing is necessary for the purposes of the legitimate interests pursued by ABS SA (Article 6(1)(f) GDPR),

8.1.3. the data subject has given consent to the processing (Article 6(1)(a) GDPR).

8.2. The DPO is responsible for the relevant provisions of the contract, referred to in Section 8.1.1, to the extent covering the requirement of protection of personal data.

8.3. Upon the first contact with a data subject, and no later than within one month from obtaining their data, ABS SA should inform the data subject of their rights under Article 14 GDPR (information clause). The scope of information is given in Appendix F.

8.4. ABS SA immediately responds to submitted legitimate data subject's requests following the information provided to them as referred to in Section 8.3.

9. Selected cases of information obligation

9.1. The information obligation, i.e. the obligation to provide the content of the information clause to the following data subjects:

- contractors–natural persons,
- employees and other persons authorized by contractors or potential contractors,

should be discharged in accordance with the guidelines of Appendix H.

9.2. As regards recruitment and employment, the rules set out in Appendix G apply.

10. Personal data processing commissioned to ABS SA

10.1. ABS SA processes personal data on commission only under a relevant contract (Personal Data Processing Agreement (PDPA)) with the commissioning party–controller or processor. The terms and conditions of such a contract should allow for the processing of personal data in line with Articles 28-29 GDPR.

10.2. Any contract referred to in Section 10.1 must include the model provisions contained in Appendix J. The above is without prejudice to the contracting procedure in place at ABS SA.

10.3. ABS SA keeps a record of PDPAs. Separate records for each product line are allowed. The Head of the Legal Department is responsible for keeping the record of PDPAs.

10.4. The record contains the information required by Article 30(2) GDPR at a minimum.

11. Personal data processing on ABS SA's commission

11.1. ABS SA commissions the processing of personal data to a processor only under the Personal Data Processing Agreement which sets out the conditions of processing that meet the requirements of Articles 28-29 GDPR.

11.2. Any contract referred to in Section 11.1 must include the basic provisions contained in Appendix K. The above is without prejudice to the contracting procedure in place at ABS SA.

12. Procedure in the event of data subject's request

12.1. The purpose of the procedure in the event of data subject's request is for ABS SA to fulfil such a request, provided that it is founded upon the provision of Article 12 GDPR. If so, ABS SA provides the data subject–in a concise, transparent, intelligible and easily accessible form, using clear and plain language–any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 GDPR relating to processing.

12.2. The DPO is responsible for the proper fulfilment and handling of requests, unless it is against the law.

12.3. The DPO uses RU to keep track of the procedure of handling each data subject's request.

12.4. The procedure of handling data subject's request is contained in Appendix C.

13. Storage limitation

13.1. The storage of personal data for a period longer than necessary for the purposes for which the data is processed is prohibited. This period is shown in the records of processing activities, according to the current status in RU.

13.2. Each owner of each domain-specific application is required to implement and follow a procedure that stops the processing of personal data to which access is granted with this application. Such a procedure should be adapted to the nature and functionality of any given domain-specific application with a view to reducing the risk of a personal data breach due to storage for a period longer than necessary for the purpose for which the data is processed.

14. Violation of the PDPP as a personal data protection breach

14.1. A personal data protection breach is an event that leads or may lead to (i) an accidental or unlawful modification (including destruction) of processed data, (ii) granting access to data to unauthorized persons or (iii) unauthorized disclosure of data. Some examples of such breaches are:

- unfounded granting of access rights,
- losing or finding a media carrier containing personal data,
- unauthorized download of personal data,
- disclosing personal data to an unauthorized person,
- loss of equipment or documents containing personal data,

- storage of paper documents improperly safeguarded against access by unauthorized persons,
- traces of tampering with or attempted forced entry to rooms or premises where personal data can be accessed.

14.2. The purpose of the procedure in the event of a personal data breach is to minimize the adverse consequences of the breach leading to damage to the data subject and to ABS SA by addressing the circumstances indicating the occurrence of the breach promptly and adequately.

14.3. Each employee is obliged to report any event or incident that may be regarded as compromising personal data safeguards. The procedure in the event of personal data protection breaches is contained in Appendix B.

15. PDPP violation other than a personal data protection breach

15.1. Violation of the PDPP that is not a personal data protection breach is an event that leads or may lead to the violation of the provisions of the GDPR but does not constitute a breach referred to in Section 14.1. Some examples of such breaches are:

- obtaining personal data from illegal sources,
- the processing of personal data unlawfully (without a legal basis),
- collection of personal data without fulfilling the information obligations;
- failure to train employees in personal data protection.

15.2. The purpose of the procedure in the event of violations of the PDPP other than a personal data protection breach is to minimize the adverse consequences of the breach leading to damage to ABS SA by addressing the circumstances indicating the occurrence of the breach promptly and adequately.

15.3. Each employee is obliged to report immediately any event or incident that may be regarded as violating the PDPP and not being a personal data protection breach. This information should be reported to the address odo@assecobs.pl along with a precise description of the event or incident.

16. Personnel training

16.1. Each employee must be trained in the protection of personal data.

16.2. The Head of the HR Department is responsible for conducting the training.

16.3. The training scope should cover the PDPP to the extent necessary for the processing of personal data, including the relevant laws and liability. A recommended training scope is provided in Section A.1.

16.4. The training closes with the participants making a statement of participation and understanding the training content and of commitment to complying with the personal data protection rules covered during the training. Such model statements are provided in Sections I.4 and I.5.

17. Data Protection Officer (DPO)

17.1. The DPO is appointed by a resolution of the Management Board of ABS SA.

17.2. As regards their performance of duties relating to ensuring the proper protection of personal data processed by ABS SA, the DPO reports directly to the Member of the Management Board who supervises the protection of personal data, or, if they are absent, to the President of the Management Board.

17.3. DPO's duties, beyond the tasks listed in Article 39(1) GDPR, cover the following:

17.3.1. to keep the PDPP up-to-date to the extent necessary to ensure the protection of personal data in relation to the current state of the art and to comply with applicable laws,

17.3.2. to submit to the Management Board messages or reports on the compliance status of the processing of personal data in the company with the provisions on the protection of personal data,

17.3.3. to keep:

17.3.3.1. a record of processing activities in accordance with Article 30(1) GDPR;

17.3.3.2. a list of domain-specific applications;

17.3.3.3. a record of personal data protection breaches;

17.3.3.4. the Tables of Access Rights for each domain-specific application;

17.3.3.5. records of activities listed in Section 17.3.4-17.3.5.

17.3.4. to communicate with data subjects in order to handle their requests to access, rectify, erase, transfer, or restrict the processing of data, or to object to its processing, and in all other matters that may be submitted by a data subject to ABS SA based on the rights granted to them under the GDPR,

17.3.5. to communicate with competent public authorities that may demand access to information about a specific data subject,

17.3.6. to keep the RU database up-to-date and consistent with the actual state of affairs,

17.3.7. to offer consultation referred to in Section 6.3,

17.3.8. to approve the provisions of contracts referred to in Sections 8.1.1, 10.1 and 11.1, in the part concerning the protection of processed personal data,

17.3.9. to approve the content of the website referred to in Section 2.4,

17.3.10. to manage and participate in auditing the proper performance of the contract referred to in Section 11.1 within the powers of ABS SA under Article 28(3)(h) GDPR.

17.4. The recording of activities referred to in Section 17.3 and of any other activities that the DPO deems justified as part of their duties is done, if not impossible, with RU.

17.5. In order to enable them to perform their duties, the DPO is entitled to:

17.5.1. put forward recommendations to the ABS SA's executives regarding the protection of personal data,

17.5.2. receive from the ABS SA's executives any information regarding the processing of personal data,

17.5.3. conduct any necessary checks to assess organizational and technical measures aimed to ensure the protection of personal data processing at ABS SA,

17.5.4. if the DPO detects a personal data protection breach, instruct the ABS SA employees to cease the breach and take other action to mitigate the consequences of any such violations.

17.6. The DPO has the right to bindingly instruct the ABS SA employees to the extent necessary for ABS SA to meet the requirements of personal data protection law.

17.7. DPO's contact details are as follows:

- e-mail address: odo@assecobs.pl,
- geographical address: Inspektor Ochrony Danych Asseco Business Solutions S.A., Konrada Wallenroda 4C, 20-601 Lublin

Appendix A. A general description of technical and organizational measures employed by ABS SA to ensure the protection of processed personal data

Basic principles:

A.1. Access to personal data can only be obtained after proper identification, authentication, and obtaining authorization to access.

A.2. The access provider is responsible for providing access only to such an access requester who has been properly identified, authenticated and has requested authorization to the extent corresponding to the performance of their duties.

A.3. The access provider is responsible for ensuring conditions to enable identification of the access requester, and the access requester is responsible for following the identification procedure so as to reduce the risk of third parties taking control over the access requester's authentication data.

Organizational safeguards:

A.4. ABS SA has appointed the DPO controlled by the Management Board (see Section 17).

A.5. ABS SA has implemented the Personal Data Protection Policy (PDPP).

A.6. Each employee is required to take part in a training on the protection of personal data–see Appendix I.

A.7. Every employee is required to report any detected instances of violation of the PDPP, in particular any cases where users run programs posing a risk of a security breach, non-compliance with the rules of using domain-specific applications or processing data in a manner that is incompatible with the personal data protection procedures described in the PDPP.

A.8. Every employee has been made familiar with the provisions on the protection of personal data, as provided in their relevant declaration. In particular, they make a declaration of commitment to keep personal data confidential (see Section I.4).

A.9. In the event of processing personal data at the request of another entity or commissioning other entity to process data, ABS SA enters into a contract that minimizes its risk as regards the likelihood of the occurrence of threats to the security of personal data and the relevance of these threats.

A.10. Within the NSP, the following procedures have been implemented:

- administration of system resources, including the maintaining of an up-to-date record of network and communication servers,
- configuration of directory services (authentication and access granting),
- reconstruction, operating continuity, including the power supply backup and air conditioning systems,
- disaster recovery of information resources,
- management of personnel access to server rooms and switching devices rooms,
- network traffic protection, including traffic monitoring and system services,
- access management using the ART,
- software updates and malware protection,

- incident monitoring and response,
- periodic safety checks and tests,

which are employed to ensure the protection of personal data.

Technical safeguards:

A.11. Personal data stored in the server room of the ABS SA's Data Processing Centre is safeguarded by the technical means at the Centre's disposal.

A.12. Personal data in a traditional form (paper form documentation), stored in the premises of ABS SA, are protected by the technical means described in the physical protection and access monitoring procedures, alarm system, anti-burglary systems, key control policy (including ID cards), etc.

A.13. The NSP provides for the following "logical" safeguards corresponding to threats and the risk of their occurrence:

- user authentication through directory and application services, including a permit hierarchy,
- separation and segmentation of computer networks,
- logging and analysis of user activity, including the analysis of system logs (SIEM),
- cryptographic protection of stored and transmitted data,
- data pseudonymization,
- validation of the quantity and quality of entered data,
- automatic notification of potential threats to domain-specific applications,
- intrusion detection systems and intrusion prevention systems (IDS/IPS),
- Business Activity Monitoring
- using programs that reduce a risk of malware damage,
- implementation and observance of the mobile device management policy,

which are employed to ensure the protection of personal data.

Appendix B. Procedure in the event of a personal data protection breach

B.1. The reporting person (see B.2 below) is required to secure the traces or evidence related to the event or incident that they consider a breach immediately after the incident and in a manner corresponding to the nature of the incident.

B.2. The procedure flow chart is given on page 15. Procedure participants:

Reporting person–a person who noticed a breach incident and reported it to the DPO or DSAA

Domain-specific application administrator

Domain-specific application owner

DPO

Management Board

B.3. Notification of a personal data breach to the supervisory authority or processor is done as follows:

B.3.1. the DPO, without undue delay and, where possible, yet not later than 72 hours after having become aware of the breach, notifies it to the supervisory authority, unless the breach is unlikely to result in a risk to violate the rights and freedoms of natural persons (condition R1 is met, see page 15). Where the notification to the supervisory authority is not made within 72 hours, reasons for the delay must be attached.

B.3.2. The DPO assesses whether condition R1 has been met.

B.3.3. If ABS SA is the processor, after becoming aware of a breach, it notifies the controller or processor within the time limit specified in the contract.

B.3.4. If, and to the extent that, the information about a breach cannot be communicated at the same time, it can be communicated gradually without undue delay.

B.3.5. The DPO records any personal data protection breaches, including the circumstances, effects and remedial action taken, in a record of personal data breaches using RU.

B.4. Article 34 GDPR sets out the procedure and scope of communication to the data subject of a personal data breach. When it comes to ABS SA, the following should be considered:

B.4.1. The DPO communicates a personal data breach to the data subject without undue delay.

B.4.2. However, if condition R2 is not met (see page 15), i.e.:

a) the breach does not pose a high risk to the violation of rights and freedoms of natural persons;

b) in the event of a breach of protection and in relation to data suffering from a breach, ABS BS implements appropriate technical and organizational measures to prevent unauthorized persons from viewing the data;

c) after the occurrence of a breach, ABS SA has implemented measures eliminating the likelihood of high risk of violation of the rights or freedoms of the data subject;

d) the communication would entail a disproportionate effort. Should this be the case, data subjects will be informed by a message on the ABS SA website or in an equally effective manner;

then, the DPO will not communicate the personal data breach to the data subject. The DPO assesses whether condition R2 has been met.

B.5. The communication to the data subject will be given in *clear and plain language* and will contain:

B.5.1. a description of the breach;

B.5.2. the name and contact details of the DPO;

B.5.3. a description of the likely consequences of the breach;

B.5.4. a description of the measures taken or proposed to be taken to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

B.6. If the DPO confirms a threat to personal data, it will carry out an investigation and will:

B.6.1. determine the scope and causes of the threat and its possible consequences in the absence of remedial action;

B.6.2. record the course of the investigation;

B.6.3. propose possible disciplinary action;

B.6.4. recommend preventive action aimed at eliminating similar threats in the future.

B.7. If the DPO confirms the occurrence of a personal data protection incident, it will carry out an investigation and will:

B.7.1. determine the time of the incident along with its scope, causes, effects and size of possible damage;

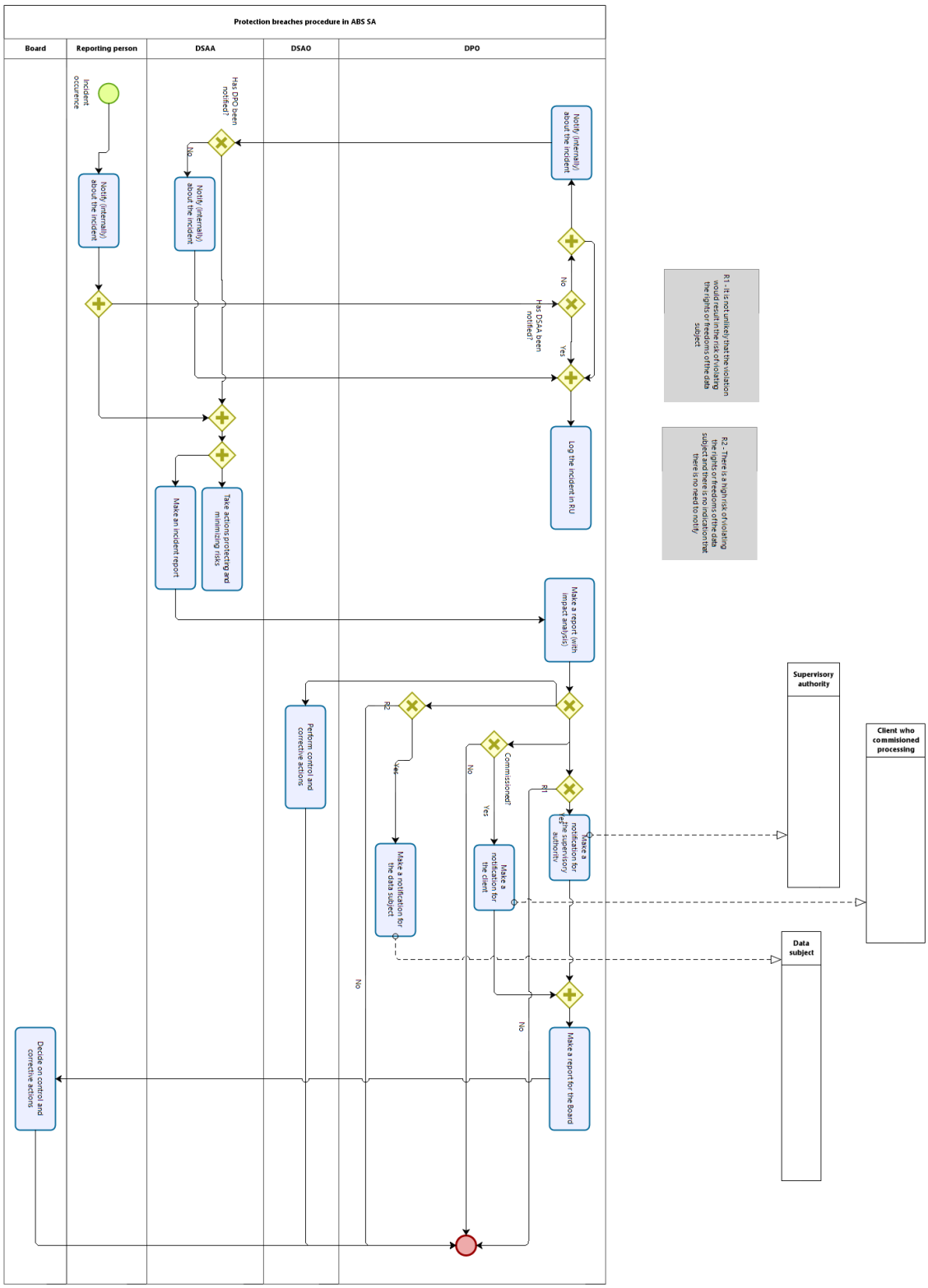
B.7.2. secure any evidence;

B.7.3. take corrective action (removing the effects of the incident and limiting damages);

B.7.4. record the course of the investigation;

B.7.5. determine the scope of responsibility for the violation of the PDPP of specific persons and will propose disciplinary action or will notify competent authorities of a possible offence;

B.7.6. recommend corrective action aimed at eliminating similar incidents in the future.


Protection breaches procedure in ABS SA
Board
Reporting person
DSAA
DSAO
DPO
Incident occurence
Notify (internally) about the incident
Has DPO been notified?
No
Notify (internally) about the incident
Notify (internally) about the incident
No
Has DSAA been notified?
Yes
Log the incident in RU
Make an incident report
Take actions protecting and minimizing risks
Make a report (with impact analysis)
R1 - It is not unlikely that the violation would result in the risk of violating the rights or freedoms of the data subject
R2 - There is a high risk of violating the rights or freedoms of the data subject and there is no indication that there is no need to notify
Supervisory authority
Client who commisioned processing
Data subject
Perform control and corrective actions
R2
Yes
Make a notification for the data subject
No
Commissioned?
Yes
Make a notification for the client
No
R1
Make a notification for the supervisory authority
No
Make a report for the Board
Decide on control and corrective actions

Appendix C. Procedure of handling data subjects' requests

C.1. The data subject may request:

- access to data and its copies,
- rectification of their personal data,
- discontinuation of processing after their objection,
- restriction of processing,
- erasure of their personal data,
- transfer of machine-readable data,
- access to machine-readable data,

in any way at their discretion, however, ABS SA will accept the request if it raises no doubts as to the data subject's intentions (Article 60 of the Civil Code). However, the simplest way to submit a request is via e-mail to the DPO's address given in Section 17.7.

C.2. ABS SA acts in response to a data subject's request having confirmed the identity of the data subject. The confirmation is made after prior verification using commonly accepted methods, i.e.:

- face comparison, that is, the comparison of data subject's appearance with the image in the presented ID–in the case of a face-to-face contact,
- by means of the e-PUAP safe profile if an electronic document is presented,
- by means of the qualified electronic signature if an electronic document is presented,
- based on identification parameters kept by ABS SA–for remote identification–if submitted by the data subject properly.

C.3. If a data subject appears in person to make a request, they will be served by a member of the reception desk personnel in accordance with the general visitor handling rules.

C.4. In the case of a face-to-face contact, identity verification is carried out by a member of the reception personnel in every ABS SA's location. The result of the verification is recorded in the request application after which it is immediately forwarded to the DPO in accordance with the handling procedure for internal communication. The result of the verification contains:

- name and surname of the verifier,
- date and time of verification,
- a clause saying:

  identity verified successfully

  or (plus the underlying reason):

  identity has not been verified successfully because _____.

C.5. If a data subject's request is made orally, they should be asked to do it in the form of: writing, recording, image, etc. If the data subject fails to make the request in any of such forms, this fact should be recorded and reported to the DPO.

C.6. In the case of remote contact, identity verification is done by the DPO based on the content of the request and using the data subject identifiers held by ABS SA[*]. The DPO may authorize another person to verify identity in the case of remote contact.

C.7. If a request is submitted to a person other than the DPO, it should be immediately forwarded to the DPO provided that:

- if a personal contact has been established, it should be done in accordance with rules C.3 and C.4,
- if a remote contact has been established, it should be done via e-mail by sending the request to odo@assecobs.pl.

C.8. If identity verification fails, in their response to the requester, the DPO refuses to fulfil the data subject's request and states the grounds for refusal.

C.9. In identity verification is successful, the DPO responds to the requester having collected the necessary information using RU and, where appropriate, other ways.

C.10. The DPO responds to the data subject within the time limits set out in the GDPR, however, at their earliest convenience.

[*] For example, if a request has been sent from an e-mail address that is stored in the ABS SA resources as registered previously, then identity should be considered verified successfully.

Appendix D. The processing of personal data based on consent

D.1. Guidelines for a consent to process

D.1.1. Each data subject may allow the data controller to process personal data related to that data subject. It is in the interest of ABS SA that such a consent raises no doubts as to the intentions of the data subject (Article 60 of the Civil Code). Such consent should not be presumed or implied based on another or different declaration of will, either. Combination of consents is not allowed. To set up "implied consent" in online forms is prohibited.

D.1.2. The data subject may give their consent in any manner. They do not have to do it using the template form proposed by ABS SA. However, in practice, the use of such template forms is recommended as they contain the wording approved by the DPO. Using the template is a guarantee that the consent complies with the law, and that ABS SA is in a position to deem it valid and binding.

D.1.3. Consent is not always required: it is merely one of the ways to legitimize the processing of personal data. The purposes of processing that do not require consent[*] are, for example, the preparation, conclusion and performance of a contract with the data subject, the marketing of own products, compliance with the requirements of recording sales, fulfilment of obligations under statutory warranty, etc. On the other hand, the purposes of processing that require consent are, for example, transfer of data to third parties (e.g. to other companies of the capital group or outside the group), the marketing of foreign products, or the use of personal data to take part in competitions. If in doubt as to whether consent is needed in given processing circumstances, refer to the DPO for advice.

D.1.4. Along with obtaining the consent, the information obligation should be fulfilled as referred to in Article 13 GDPR and described in Appendix E. For this reason, it is recommended that information clauses be included in the consent form as its integral part.

D.1.5. Consent can be obtained through the application (browser) dialogue interface, as long as a legible layout and integrity of the information clauses are maintained.

[*] A dividing line should be drawn between the consent of a data subject to the processing of their personal data and their consent to receiving commercial information by electronic means, or the consent to the use by ABS SA of telecommunications terminal equipments used by the data subject for the purposes of direct marketing. Such consents do not fall under the PDPP and are not consents within the meaning of the GDPR.

Appendix E. Information about the processing of personal data–data obtained directly

E.1. When ABS SA collects personal data, it is necessary to provide the data subject with such information that will allow them, if necessary, to take action to exercise their right to privacy. In the exercise of this right, they may, for example, request that the data collection be ceased or, at a later date, that the data be rectified or erased.

E.2. When obtaining data directly from the data subject, the information listed below should be provided but only *when* and to the extent to which the person does not have them yet. In ABS SA's practice, however, it means: during the first contact with the person.

E.3. The whole process can be carried out in any form, for example, via a web browser form, in the introduction to the first e-mail to that person, etc., as long as a legible layout as well as the integrity of information clauses are essentially maintained.

E.4. In the case of direct collection of personal data, the information clause contains the following elements:

		Clause-specific content
	O	ABS's contact details:
	O	contact details of the Data Protection Officer in ABS
	O	the purpose of processing and the legal basis
		if the basis for processing is ABS's legitimate interest, a description of this interest
	U1	information on the categories of recipients, if any
	U2	information on the intention to transfer personal data to a third country
D	O	retention period. Time limits may be provided or a method of defining time limits
	O	information about the right to request access to personal data, its transfer, rectification, erasure or restriction of processing, as well as the right to submit an objection to processing, effective from the moment of submission, unless ABS SA demonstrates the existence of legally valid grounds to continue the processing that override the interests, fundamental rights and freedoms of the data subject, or grounds to determine or claim damages or defend against claims, excluding the objection to processing for marketing purposes
D		if the processing takes place based on data subject's consent, information about the right to withdraw the consent along with a statement that the withdrawal of consent does not affect the lawfulness of processing done before the withdrawal
	O	information about the right to lodge a complaint to the supervisory body
D	O	information whether the provision of data is a statutory or contractual requirement or a condition for the conclusion of a contract, and whether the data subject is obliged to provide it, and what are the possible consequences of failure to do so

	O	information on automated decision-making, including profiling, and any relevant information about the decision-making rules as well as on the significance and envisaged consequences of such processing for the data subject
		information about the intention of further processing for purposes other than the purpose for which the personal data has been collected, including the information on the other purpose and information referred to in the D rows above

Explanation

O–obligatory clause

U1–In order to provide the information about the categories of data recipients correctly, the recipient should be considered any person or company or authority to whom personal data is disclosed. In the event of disclosure of data to public authorities that may receive personal data *in the framework of a particular inquiry*, such authorities are not regarded as recipients. Thus, for example, disclosure of the personal data of the contractor's contact person in the course of investigation conducted by law enforcement agencies does not entail the obligation to point to such agencies as recipients.

U2–If personal data were to be transferred to a third country, prior to collecting such data, it is necessary to consult the content of the clause with the DPO.

Appendix F. Information about the processing of personal data–data obtained indirectly

F.1. When ABS SA processes personal data, it is necessary to provide the data subject with such information that will allow them, if necessary, to take action to exercise their right to privacy. In the exercise of this right, they may, for example, request that the data collection be ceased or that the data be rectified or erased.

F.2. ABS SA provides only such information that the person does not have. In ABS SA's practice, however, it means: during the first contact with the person. However, this information should be provided no later than within one month from the obtaining of personal data.

F.3. The whole process can be carried out in any form, for example, in the introduction to the first e-mail to that person, as long as a legible layout as well as the integrity of information clauses are essentially maintained.

F.4. In the case of indirect collection of personal data, the Information Clause contains the following elements (see the explanation in Appendix E):

	Clause-specific content
O	ABS's contact details:
O	contact details of the Data Protection Officer in ABS
O	the purpose of processing and the legal basis
	if the basis for processing is ABS's legitimate interest, a description of this interest
O	information on the source of data
O	enumeration of personal data categories
U1	information on the categories of recipients, if any
U2	information on the intention to transfer personal data to a third country
O	retention period. Time limits may be provided or a method of defining time limits
O	information about the right to request access to personal data, its transfer, rectification, erasure or restriction of processing, as well as the right to submit an objection to processing, effective from the moment of submission, unless ABS SA demonstrates the existence of legally valid grounds to continue the processing that override the interests, fundamental rights and freedoms of the data subject, or grounds to determine or claim damages or defend against claims, excluding the objection to processing for marketing purposes
	if the processing takes place based on data subject's consent, information about the right to withdraw the consent along with a statement that the withdrawal of consent does not affect the lawfulness of processing done before the withdrawal

O	information about the right to lodge a complaint to the supervisory body
O	information on automated decision-making, including profiling, and any relevant information about the decision-making rules as well as on the significance and envisaged consequences of such processing for the data subject

Appendix G. The processing of personal data for recruitment and employment purposes

In this Appendix, "employee" refers to a person employed under a contract of employment.

G.1. The processing of personal data for recruitment purposes

G.1.1. When ABS SA processes personal data for recruitment purposes, the basis for processing is the legitimate interest of ABS SA. However, ABS SA may lawfully require the candidate to provide only such personal data that falls within the following categories:

- name and surname;
- date of birth;
- contact details (though the candidate may share only the contact details of their choice),

and also, when it is necessary for the employment of a particular type or in a specific position:

- completed education;
- professional qualification,
- employment history.

G.1.2. All other data, except for that mentioned in Section G.1, may be collected by ABS SA only based on the candidate's consent.

G.1.3. When collecting data, ABS SA is obliged to comply with the information obligation by providing the candidate with the following information:

> The controller of your personal data is Asseco Business Solutions SA, seated in Lublin (Poland), at ul. Konrada Wallenroda 4C, (KRS 28257).
>
> Your data shall be processed by ABS in the recruitment procedure that you have joined by submitting the application documents, i.e. based on Article 6(1)(c) GDPR, which provides that processing is necessary for compliance with a legal obligation to which the controller is subject.
>
> The law requires that you should provide the following personal data for recruitment purposes:
>
> - name and surname;
> - date of birth;
> - contact details;
> - completed education;
> - professional qualification;
> - employment history.
>
> The provision of other data is voluntary. By pressing Submit, you agree to the processing of any other personal data that you have included in your recruitment application. This consent covers additional personal data that has not been addressed in the relevant law, e.g. your image. ABS needs such a consent in accordance with Article

6(1)(a) GDPR in order to process this data legally. So, if you do not want ABS to process any additional data about you, do not disclose it in your documents.

Your personal data shall be processed until the end of the recruitment procedure that you have joined by submitting your application documents, or, if you have agreed to take part in future recruitment procedures, for the period indicated therein or until your consent is withdrawn.

You have the right to withdraw your consent at any time, yet, this shall not affect the lawfulness of processing that shall have been done until the withdrawal.

You shall have the right to request ABS, at any time, to enable you to access your personal data and to transfer, rectify, erase or restrict the processing of your personal data.

You shall also have the right to object to the processing of your personal data. Having received your objection, ABS shall no longer be able to process your personal data unless it proves that there are (i) legally valid grounds to continue the processing that override your interests, fundamental rights and freedoms, or (ii) grounds to determine or claim damages or defend against claims.

You shall have the right to file a complaint to the supervisory authority, i.e. Prezes Urzędu Ochrony Danych Osobowych (the President of the Personal Data Protection Office), when, in your opinion, the processing of your personal data violates the provisions on the protection of personal data.

ABS may share the collected personal data with entities cooperating with ABS to the extent necessary to handle recruitment procedures.

Under no circumstances shall ABS use your data for automated decision-making that may affect your legal situation.

If you need to contact ABS on the matter of protection of your personal data, you can do so by writing to the address of our Data Protection Officer: odo@assecobs.pl or to ABS's mailing address given in the opening sentence.

Yours sincerely,
Asseco Business Solutions SA

G.1.4. Given the common practice of candidates disclosing in their CVs also other data than required by the law for the recruitment process, a model of candidate's consent has been drawn up as follows:

☐ I hereby give my consent to Asseco Business Solutions SA, seated in Lublin, 20-607, at ul. Konrada Wallenroda 4C, company registration no. KRS 28257, to the processing of my personal data contained in the application (the form and the attached recruitment documents) in order to conduct future recruitment procedures, however, for no longer than for 2 years from the date of this consent.

G.1.5. If need be, ABS SA may request the candidate to consent to processing for an indefinite period of time.

G.1.6. If the candidate gives their consent using a text or form other than the proposed model form given in G.1.4, ABS SA will respect the candidate's choice. This will not put the candidate in an inferior position in the recruitment process and, specifically, will not give grounds to refuse their application or possible employment.

G.1.7. The Head of the HR Department is responsible for collecting the candidate's consent and fulfilling the information obligation. The performance of the obligation can be satisfied using the eRecruiter domain-specific application.

G.2. The processing of personal data for employment purposes

G.2.1. In the case of processing personal data by ABS SA in order to conclude a contract of employment with a candidate and with an employee, the basis for processing is the legitimate interest of ABS SA and activities necessary to perform the contract with the data subject as a party (Article 6(1)(b) GDPR). However, ABS SA may lawfully require an employee to provide only such personal data that is listed in Section G.1.1and:

- personal identification number PESEL or, in its absence, the type and number of another document confirming the identity;
- address of residence,
- and–*only when providing such data is* necessary *on account of the employee being entitled to special rights under labor law*–other employee's data and also the personal data of the employee's children and other close relatives;
- and–*only when it is deemed* indispensable *for the employer to fulfil its legal obligation*–other employee's personal data.

G.2.2. Any other data, except for that mentioned in Section G.2.1, may be collected by ABS SA based on its legitimate interest or pursuant to the employee's consent. The categories of this data are listed in Section G.2.3.

G.2.3. When collecting data, ABS SA is required to meet its information obligation by providing the employee with the following information:

The controller of your personal data is Asseco Business Solutions SA, seated in Lublin, at ul. Konrada Wallenroda 4C (KRS 28257).

Your data is and shall be processed by ABS for the following purposes:

- to establish an employment relation and perform the contract of employment that you are a party to, i.e. based on Article 6(1)(b) of the General Data Protection Regulation (GDPR),
- for compliance of ABS with a legal obligation to which it is subject, i.e. the provisions of labor law, social security and social protection, as well as for billing, tax and book-keeping purposes, i.e. based on Article 6(1)(c) GDPR,
- to perform contracts concluded with ABS's contractors that you shall be involved in, to secure premises and access to information resources, and to determine or claim damages or defend against damages, i.e. to pursue ABS's legitimate interests based on Article 6(1)(f) GDPR,

- to handle tasks that need your personal data for effective execution and to offer you additional, non-statutory benefits related to employment (e.g. taking advantage of additional and non-mandatory benefits and services offered by ABS)–upon your separate and voluntarily consent, i.e. based on Article 6(1)(a) GDPR.

You shall provide your personal data to the extent that is required by the law, and, in particular, to the extent necessary for employment purposes, the performance under the contract of employment, compliance with the obligations under labor law or other relevant rules and regulations, including the provisions on social security and social protection. Failure to provide such data shall prevent the conclusion or performance of the contract of employment as well as meeting the obligations under the law.

You shall provide your personal data to the extent necessary to ensure security on ABS's premises and to control access to locations where work is performed. Failure to provide such data shall render access to our facilities or premises impossible.

To the extent that your personal data is processed to enable the exercise of your rights under labor law or granted by ABS, providing personal data is voluntary, yet failure to provide it shall render your rights void.

Your personal data shall be processed for the following periods:

- for performance under a contract of employment–no longer than until the expiration or termination of the contract,
- for purposes related to legitimate interests–until making an objection to processing,
- for compliance of ABS with a legal obligation to which it is subject–until the deadline provided for in the law,
- if you have given additional consent–until you withdraw it. However, the withdrawal shall not affect the lawfulness of processing that shall have been done based on your consent before its withdrawal,

–while these periods can be prolonged by the time necessary to claim damages or defend against claims.

You shall have the right to request ABS, at any time, to enable you to access your personal data and to transfer, rectify, erase or restrict the processing of your personal data.

You shall also have the right to object to the processing of your personal data to the extent that the processing is done order to pursue ABS's legitimate interests. Having received your objection, ABS shall no longer be able to process your personal data unless it proves that there are (i) legally valid grounds to continue the processing that override your interests, fundamental rights and freedoms, or (ii) grounds to claim damages.

ABS may share the collected personal data with the tax authority, the competent body in matters of sickness benefits, the competent body in matters of public healthcare, the pension authority and debt collectors.

You shall have the right to file a complaint to the supervisory authority, i.e. Prezes Urzędu Ochrony Danych Osobowych (the President of the Personal Data Protection Office), when, in your opinion, the processing of your personal data violates the provisions on the protection of personal data.

If you need to contact ABS in matters relating to the protection of your personal data, please, contact ABS's Data Protection Officer at: odo@assecobs.pl.

Asseco Business Solutions SA

I hereby declare that on _____ [1] _____ I have read the above information.

_____[5]_____
_____[2]_____

G.2.4. In addition, in order to enable the processing of employee's personal data whose collection is not legitimate under applicable law, but such data is needed for the effective operation of the internal communication system, ABS SA will secure the consent of the following content:

Relative to the contract of employment dated _____ [3] _____ concluded between me and Asseco Business Solutions SA, I hereby give my voluntary consent to the employer's processing of my image for the purposes of the internal communication system.

Date _____[4]_____

_____[5]_____
_____[2]_____

Failure to give, or withdrawal of, the consent referred to above shall not disadvantage you in any way whatsoever or be the basis for unfair treatment, nor shall it entail any negative consequences; in particular, it shall not give grounds to termination of the contract of employment or its termination without notice. However, it shall disadvantage ABS in pursuing tasks that require your personal data for effective performance.

Asseco Business Solutions SA

where:

[1]–the date of making the declaration by the employee

[2]–employee's signature

[3]–effective date of the contract of employment

[4]–date of employee's consent

[5]–employee's name and surname

G.2.5. If the employee does not give their consent requested by ABS SA, ABS SA will respect their choice. This will not disadvantage the employee in any way or justify their unfair treatment and will not cause any negative consequences; in particular, it will not give grounds to termination of the contract of employment or its termination by ABS SA without notice.

G.2.6. The Head of the HR Department is responsible for fulfilling the information obligation and collecting the consent referred to in Section G.2.4. To prove that the obligation has been met, relevant records and documents should be attached to the employee personal file.

Appendix H. Routine performance of the information obligation

H.1. Each employee of ABS SA who, when performing their duties (or contract), collects personal data of contractors who are natural persons or natural persons empowered by contractors or potential contractors is obliged to inform such persons of the processing of their personal data.

H.2. This information should be provided at the first contact with the data subject, and not later than within one month if the data has been collected indirectly (e.g. from the public domain).

H.3. In order to facilitate the fulfilment of the information obligation, a uniform information clause (**UIC**) has been adopted covering as many cases from the ABS SA's business practice as possible. The UIC is as follows:

Due to the requirements of the General Data Protection Regulation (**GDPR**, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016), please, be advised that ABS processes your personal data.

Asseco Business Solutions SA, seated in Lublin, at ul. Konrada Wallenroda 4C, (KRS 28257) becomes the data controller upon their receipt.

You can contact our Data Protection Officer by traditional mail by writing to the address given above or by electronic mail at odo@assecobs.pl.

Your data may be processed by ABS for the following purposes:

- to contact you in relation to contracts you are not a party to but your personal data has been obtained by ABS in connection with their performance,
- to enable ABS to carry out a direct marketing of its products and services, including–if you so consent–the sending of commercial information by electronic means (e.g. invitations to ABS's events or information about ABS's products and services),
- to determine damages, claim damages or defend against claims,
- to monitor and enhance of the quality of provided services, including the handling of complaints,

i.e. based on Article 6(1)(f) GDPR, that is, on our legitimate interest, in which case you have the right to object to processing; your objection shall be effective from the time of its submission as regards marketing purposes while in other cases it shall be valid unless we prove the existence of legally valid grounds to continue the processing that override your interests, fundamental rights and freedoms or prove grounds to determine or claim damages or defend against claims,

or

- to comply with a legal obligation (compliance with the laws), including for accounting and tax purposes and in connection with the book-keeping operations, i.e. based on Article 6(1)(c) GDPR,

or

- to perform a contract that you are or may be a party to; or to take steps, upon your request, before entering into such a contract, such action including the provision of services to you, to maintain your account in one of our services, i.e. based on Article 6(1)(b) GDPR.

ABS intends to keep your data for the above-listed purposes and for no longer than necessary to achieve them, that is:

- in relation to the processing of your personal data in connection with the performance of an agreement that you are a party to–for the term of such an agreement,
- in relation to the processing of your personal data for the purpose of direct marketing of ABS's products and services–until the date of your objection to process your personal data.

After this time, the data shall be stored for purposes, to the extent and for as long as required by the law or to determine damages, claim damages or defend against claims.

You shall have the right to request ABS, at any time, to enable you to access your personal data and to transfer, rectify, erase or restrict the processing of your personal data.

You shall also have the right to object to the processing of your personal data. Having received your objection, ABS shall no longer be able to process your personal data unless it proves that there are (i) legally valid grounds to continue the processing that override your interests, fundamental rights and freedoms, or (ii) grounds to determine or claim damages or defend against claims.

You shall have the right to file a complaint to the supervisory authority, i.e. Prezes Urzędu Ochrony Danych Osobowych (the President of the Personal Data Protection Office), when, in your opinion, the processing violates the provisions on the protection of personal data.

In the case of obtaining personal data from you, its submission may be required for the conclusion of, and performance under, an agreement concluded with you. Failure to submit your personal data shall prevent the conclusion of, or performance under, an agreement concluded between you and ABS. In some cases, the law may impose on ABS an obligation to obtain your personal data, e.g. for tax or accounting purposes. In other cases, submission of your personal data shall be voluntary but failure to do so may make it impossible to serve the purposes listed above (e.g. ABS will not be able to send you any communication about its products).

ABS processes the following categories of personal data:

> Your name and surname and any of the following categories: e-mail address, telephone number, geographical address, and–if a contract has been concluded–the relevant identifier, such as personal identification number PESEL or tax identification number NIP

– in any case, the processing shall be restricted only to data that is necessary to achieve a given purpose.

ABS has obtained your personal data directly from you or through another entity that ABS cooperates with or from the public domain (e.g. Centralna Ewidencja i Informacja o Działalności Gospodarczej–CEIDG i.e. the Central Records and Information on Sole Traders).

ABS may make the collected personal data available to its business partners, customers and other entities contracted by ABS as well as to banks, authorities supervising public health services, and debt collectors–always to the extent relevant for the purpose of processing, in particular regarding the performance of an agreement that you are a party to or under which you are rendered services by ABS.

Under no circumstances shall ABS use your data for automated decision-making that may affect your legal situation.

Yours Faithfully,

Asseco Business Solutions SA

H.4. The UIC is available at assecobs.pl/RODO.

H.5. The following methods of UIC handover are established:

H.5.1. in the case of personal or telephone contact, the data subject should be informed that personal data is collected by Asseco Business Solutions SA, and that its processing rules are given at assecobs.pl/RODO,

H.5.2. in the case of e-mail contact, a signature should be used in which under the ABS SA footer, there is the following message attached:

The controller of your personal data is Asseco Business Solutions SA. Information on the purpose of the processing of your personal data and on what rights you can exercise in conjunction with the processing can be found at assecobs.pl/RODO.

Appendix I. Personnel training

A.1. Each employee is required to be conversant with the following documents:

- Personal Data Protection Policy w Asseco Business Solutions SA (Personal Data Protection Policy in Asseco Business Solutions SA),
- „Polityka Ochrony Danych Osobowych" ("Personal Data Protection Policy") webcast.

The trainee confirms that they have read these documents, which is tantamount to having completed the training in the rules of personal data processing.

I.1. Each employee submits an Employee Declaration to demonstrate that they have become familiarized with the rules personal data processing to the extent required by ABS.

I.2. The Head of the HR Department is responsible for collecting such declarations.

Employee Declaration: contract of employment

I.3. The declaration is stored in the employee personal file.

I.4. Below there is a model declaration of a person employed under the contract of employment:

EMPLOYEE DECLARATION

I, the undersigned, _____ (Employee), declare that I am familiar with the rules of processing personal data to the extent required by Asseco Business Solutions SA (Employer) to perform the processing, as provided in the Personal Data Protection Policy (PDPP).

At the same time, I confirm that I have understood that, regardless of the content of the PDPP, I am, within universally binding law, obliged to comply with the law as it is on the date of processing, in particular with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection natural persons with regard to the processing of personal data (GDPR).

Furthermore, I confirm that I am aware that I am aware of the legal obligation to keep confidential the personal data that I receive and the methods of its safeguarding and undertake to be bound by the above obligation with regard to keeping personal data confidential.

I undertake to report to the DPO any detected instances of violation of the PDPP, in particular any cases where users run programs posing a risk of a security breach, non-compliance with the rules of using domain-specific applications or processing data in a manner that is incompatible with the personal data protection procedures described in the PDPP.

I acknowledge that any conduct contrary to the above obligation may be considered by the Employer a serious breach of employee duties within the meaning of Article 52§1(1) of the Labor Code.

Employee's signature	Date of Declaration

Employee Declaration: service contract

I.5. The declaration is kept by the HR Department.

I.6. Below there is a model declaration for a dependent subcontractor:

The Contractor declares that they are familiar with the rules of processing personal data to the extent required by Asseco Business Solutions SA (Principal) to perform the processing, as provided in the Personal Data Protection Policy (PDPP). At the same time, the Contractor confirms that, regardless of the content of the PDPP, they are, within universally binding law, obliged to comply with the law as it is on the date of processing, in particular with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection natural persons with regard to the processing of personal data (GDPR). The Contractor undertakes to keep confidential and not to disclose to third parties any personal data provided to them during the performance of the contract concluded with the Principal. The Contractor is required to report to the DPO any detected instances of violation of the PDPP, in particular any cases where users run programs posing a risk of a security breach, non-compliance with the rules of using domain-specific applications or processing data in a manner that is incompatible with the personal data protection procedures described in the PDPP. Due to the fact that for the proper performance of the service contract between the Contractor and the Principal, it shall be necessary to grant the Contractor access to personal data processed by the Principal, the Contractor declares that: • in the event that they fail to comply with the above declarations and assumed obligations, the Principal shall have the right to regard it as a material breach of the obligations under the said service contract that shall provide grounds for termination, including a material cause of termination within the meaning of Article 746 of the Civil Code, • in the event of damage to the Principal as a result of Contractor's conduct contrary to the above declarations and assumed obligations, the Principal shall have the right to demand the Contractor to repair the damage on general terms.
Contractor _____
Signature _____
Date of Declaration _____

Appendix J. A model Agreement to Process Personal Data by ABS SA at the controller's request

J.1. The model agreement contained in J1 Contract exhibit should be used.

J.2. The content of the agreement for a given client must be adapted to the specific circumstances by the person responsible for business contacts with the client.

Appendix K. A model Agreement to Process Personal Data by a processor on behalf of ABS SA

K.1. The model agreement contained in K1 Contract exhibit should be used.

K.2. The content of the agreement for a given client must be adapted to the specific circumstances by the person responsible for business contacts with the contractor.