PERSONAL DATA PROTECTION POLICY OF CENTRANS SP. Z O.O.

with its registered office in Poznań

Poznań, dated 25 May 2018

This Personal Data Protection Policy stipulates the principles of protection, system security management and the principles of processing personal data, the Controller of which is **CENTRANS Sp. z o.o.** with its registered office in Poznań (60-115), ul. Poniecka 4, registered in the District Court Poznań- Nowe Miasto i Wilda in Poznań, VIII National Court Register Division under number 0000686280, Tax No 783-176-19-75, REGON No 367779683 with a share capital of PLN 50,000.00 (say: fifty thousand zlotys) within the scope of its business activity.

I. General provisions

1. The Controller shall take any and all measures to ensure the protection of the personal data processed.
2. Taking into account the nature, scope and purposes of personal data processing, as well as the risk of infringement of the rights and/or freedoms of natural persons, this Personal Data Protection Policy implements appropriate technical, physical and organisational measures to effectively protect the personal data processed and to meet the requirements imposed by law, including the GDPR.
3. This Personal Data Protection Policy defines the Company's data protection mechanisms, policies and procedures and applies to all personal data processed by the Company.
4. All persons who have access to or use the Company data, in particular employees and associates, shall be familiar with this Personal Data Protection Policy.
5. Other documents governing data protection at the Company are as follows:
   - Principles for managing personal data processing consents,
   - Data protection breach management,
   - Principles for the exercise of the rights of data subjects,
   - Model personal data processing authorisation,
   - Data protection impact assessment procedure.

II. Glossary of definitions, terms and abbreviations

COMPANY	**OF CENTRANS SP. Z O.O.**
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
ISMS	Information Security Management System
ISA	Information Security Administrator
Controller	the authority, organisational unit, entity or person who decides on the purposes and means of personal data processing - **CENTRANS Sp. z o.o.**
PDPO	Personal Data Protection Officer - a person appointed by the Personal Data Controller to supervise the compliance with the principles and requirements of personal data protection as set out in the GDPR and national law.
PPDPO	President of the Personal Data Protection Office, a national authority that supervises the personal data protection.

PERSONAL DATA	Pursuant to Article 4(1) of the GDPR personal data mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
SPECIAL CATEGORIES OF PERSONAL DATA	Sensitive data are data that reveal a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person or data concerning that person's health, sexuality or sexual orientation.
FILING SYSTEM	Any structured set of data of a personal nature that is accessible according to specific criteria, regardless of whether that set is distributed or functionally fragmented.
PERSONAL DATA PROCESSING	By processing, the GDPR defines an operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
PROCESSOR	A natural or legal person, public authority, entity or other body that processes personal data on behalf of the Controller.
PERSONAL DATA BREACH	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
RIGHT OF ACCESS BY THE DATA SUBJECT	The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the information set forth in this section.
RIGHT TO RECTIFICATION	The data subject shall have the right to obtain from the Controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
RIGHT TO ERASURE ("RIGHT TO BE FORGOTTEN") AND RIGHT TO RESTRICTION OF PROCESSING	The data subject shall have the right to obtain from the Controller the erasure of personal data concerning him or her without undue delay and the Controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: **a)** the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; **b)** the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; **c)** the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant

	to Article 21(2); **d)** the personal data have been unlawfully processed; **e)** the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; **f)** the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
RIGHT TO DATA PORTABILITY	The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Controller without hindrance from the Controller to which the personal data have been provided, where: **a)** the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and **b)** the processing is carried out by automated means.
RIGHT TO OBJECT	The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The Controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
AUTOMATED INDIVIDUAL DECISION-MAKING, INCLUDING PROFILING	The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. "Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
PSEUDONYMISATION	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.
PROFILING	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
CONSENT OF THE DATA SUBJECT	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
INTERNAL DATA COMMUNICATION NETWORK	The Controller's Network, connecting at least two individual computer workstations, that allows users specific access to data, including personal data.

III. Purposes and scope of application

1. The purpose of the Personal Data Protection Policy shall be as follows:

- Introducing a system to protect personal data by securing them adequately according to risks and identified threats;
- Complying with legal requirements and guidelines in the area of personal data protection, in particular 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;
- Indicating principles and rules of conduct so that the Controller can properly perform his/her data protection tasks.

2. The Personal Data Protection Policy shall refer to:

- any person with access to that personal data;
- the Company's employees who process personal data;
- the Company's associates who process personal data;
- other companies with which the Company enters into personal data processing agreements.

IV. Personal data protection principles

1. Persons processing the Company's personal data shall protect the personal data being processed and exercise the rights of the data subjects.

2. The Data Subjects whose personal data are processed and transferred for processing under this document shall have the following rights:

1) the right of access to data,
2) the right to be informed,
3) the right to rectification,
4) the right to restrict data processing,
5) the right to erasure ("right to be forgotten"),
6) the right to data portability,
7) the right to object.

The rules for the exercise of the above rights are described in the principles for the exercise of the rights of data subjects.

3. The protection of personal data is implemented through organisational and physical safeguards, system software, application and users that are proportionate and adequate to the risk of a security breach of the personal data processed.

4. The safeguards in place are designed to maintain the security of personal data at the Company and to ensure that personal data have the following characteristics:

1) information availability - means ensuring that authorised persons have access to information and related resources when needed,
2) data confidentiality - means that data are not made available to unauthorised persons,
3) data integrity - means that personal data have not been altered or destroyed in an unauthorised manner,
4) data accountability - means that a person's actions can be attributed unambiguously only to that person,
5) system integrity - means the inviolability of the system, the impossibility of any manipulation, whether intentional or accidental,

6) risk management - means the process of controlling, identifying, and minimising or eliminating security risks that may affect information systems used to process personal data.

5. The personal data processed by the Company shall be:

1) collected for specified, explicit and legitimate purposes (principle of minimising personal data to the necessary content);

2) processed in a manner that ensures appropriate security of personal data;

3) protected by appropriate technical, physical or organisational measures against unauthorised, unlawful processing, accidental loss, destruction, disfigurement or damage;

4) not processed in a manner incompatible with the purpose for which they were collected;

5) limited to what is necessary for the purposes for which they are processed;

6) processed lawfully in a transparent, clear and comprehensible manner for the data subject;

7) correct and updated or reduced as necessary;

8) stored in a form which allows the data subject to be identified;

9) kept for no longer than is necessary for the purposes for which the data are processed.

6. The processing of personal data shall only be possible if at least one of the following requirements is observed:

1) processing is necessary for the fulfilment of the Company's legal obligation;

2) processing is necessary for the performance of a task carried out in the public interest;

3) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

4) processing is necessary to take steps at the request of the data subject prior to entering into a contract;

5) the processing is necessary for the performance of a contract to which the data subject is a party;

6) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

7) processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

7. The Company shall implement appropriate technical, physical and organisational measures to ensure that only those personal data are collected and processed that are necessary to achieve the specific purpose of the processing. This obligation shall also apply to the retention period of personal data.

8. An unauthorised party is deemed to be a party who has not been authorised, consented or entrusted by the Controller to access personal data.

9. Any records kept by the Controller, or on its behalf by others, shall be made available to the supervisory authority upon request.

V. Division of responsibilities

1. As a result of conducting an audit in the scope of security of personal data processing in the Company, it was recognized that, CENTRANS Sp. z o.o. is not obliged to appoint the Data Protection Officer, and therefore it is the responsibility of the Company's Management Board or the Management Board's designee for the GDPR matters:

1) supervising the organisation of the security and protection of personal data in accordance with the requirements of the GDPR and national data protection legislation;

2) contacting the data protection supervisory authority;

3) contacting the data subjects;

4) ensuring that data are processed in accordance with the principles of the Personal Data Protection Policy and other internal documents of the Company;
5) supervising the process of granting authorisations to process personal data;
6) keeping a register of processing activities;
7) keeping a register of applicable model consents for the processing of personal data and information obligations;
8) keeping a register of persons authorised to process personal data;
9) coordinating the exercise of the rights of data subjects;
10) supervising the implementation of employees' data protection rights;
11) conducting an investigation in the event of a personal data breach;
12) initiating and undertaking measures to improve the protection of personal data;
13) reviewing data protection documents at least once a year and making changes, if necessary;
14) controlling individual departments of the Company with regard to compliance of data processing with data protection regulations;
15) supervising the IT Specialist for compliance with the Company's internal personal data protection rules and regulations;
16) commissioning an GDPR compliance audit from an external company or an external Data Protection Officer to obtain an annual report on the operation of the Company's data protection system.

2. The IT specialist's data protection responsibilities include as follows:
1) conducting ongoing monitoring of the operation of the IT system and databases;
2) carrying out installation and configuration of network and server hardware and system and network software;
3) ensuring the ongoing operation of the IT system and databases;
4) optimising IT system performance;
5) managing licences, their procedures;
6) implementing the IT security measures established as part of the personal data protection system;
7) carrying out antivirus preventive measures;
8) managing backup copies of system and network software configurations;
9) managing backup copies of personal data and resources for processing them;
10) configuring and administering system, network and security software to protect data from unauthorised access;
11) supervising the security of data of persons using the Company's websites;
12) supervising the provision of emergency power supply for computers and other equipment affecting the data processing security;
13) countering attempts to breach information security;
14) granting, at the request of the Controller, designated access rights to the information in the system concerned;
15) providing the Controller with petitions for improving/changing security procedures and security standards;
16) maintaining a password policy on business equipment;
17) cooperating with suppliers of services and network and server equipment.

3. The responsibility of employees and associates, as well as all persons processing personal data shall be as follows:
1) identifying the entrustment of the processing of personal data under contracts made with outsourced entities;
2) selecting appropriate protection measures for the data being processed;
3) ensuring the security and accuracy of the personal data processed;

4) reporting any data protection breaches in accordance with the Breach Management Procedure;
5) exercising the rights of data subjects.

VI. Authorisations to process personal data

1. Pursuant to Article 29 of 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 (GDPR), the processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the Controller, unless required to do so by Union or Member State law.
2. The Controller or a person authorised on his/her behalf shall grant authorisations for the processing of personal data to all persons who process the Company's personal data, this includes persons employed under an employment contract, civil law contract, trainees and interns.
3. By granting the authorisation, the Controller shall familiarise the person concerned with the Company's data protection rules and regulations.
4. The authorisation shall be made in writing in duplicate and signed by both the authorised person and the Controller.
5. One copy of the authorisation shall be given to the person to whom the document relates and the other shall be kept in the employee's personnel file in Part B or in a record kept by the Human Resources Department.
6. The authorisation shall cease to be effective upon termination or expiry of the agreement on which the relationship between **CENTRANS Sp. z o.o.** and the authorised person is based or upon revocation of the authorisation in question.
7. The authorisation may be revoked at any time.

The Company has a model authorisation.

VII. Information obligation

1. Where personal data relating to a data subject are collected from the data subject, the Controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
   1) the identity and the contact details of the Controller and, where applicable, of the Controller's representative;
   2) contact details of the person who has been appointed for GDPR matters (if you have the Data Protection Officer this should be the details of this officer);
   3) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
   4) where the processing is based on point (f) of Article 6(1) of the GDPR, the legitimate interests pursued by the Controller or by a third party;
   5) the recipients or categories of recipients of the personal data, if any;
   6) the fact that the Controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the Controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

1) the existence of the right to request from the Controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

2) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

3) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2) of the GDPR, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

4) the right to lodge a complaint with a supervisory authority;

5) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

6) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the Controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the Controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Where data are collected from sources other than the data subjects, the data subject shall be informed without delay, at the latest within 30 days, to the extent indicated in paragraphs 1 and 2 above, as well as of the source of the personal data.

5. The Management Board or its designee shall keep a register of the applicable model consents for the processing of personal data and information obligations.

VIII. Principles of consent

1. The consent for the processing of a data subject's personal data shall be given in a documentable form (this applies whether the consent is in paper, oral (given, for example, during a telephone conversation) or electronic form).
2. Consents shall be stored in such a way that it is possible to demonstrate their possession by the Controller (principle of data accountability), as well as to perform operations on them (limiting, updating, deleting, transferring, granting access).
3. The consent shall be drafted in a clear and simple manner.
4. Giving consent shall require the activity of the person giving it.
5. If the processing of personal data is not necessary for the performance of the contract, the performance of the contract cannot be made conditional on consent.
6. The person whose data is processed on the basis of consent shall be informed at the time of collection of consent of the possibility to withdraw it at any time.
7. The withdrawal of consent shall be as simple as giving it.
8. The Management Board or its designee shall keep a register of the applicable model consents for the processing of personal data and information obligations.

IX. Processors

1. Where the processing of personal data is to be carried out on behalf of **CENTRANS Sp. z o.o.**, the services of entities shall be used that ensure that the means of communication used to collect, receive, transmit and store the data guarantee their protection against access by unauthorised third parties and against accidental loss, destruction, distortion and damage to the personal data.
2. Processors shall guarantee the implementation of appropriate technical and organisational measures so that the processing complies with the GDPR requirements and this Personal Data Protection Policy and protects the rights of data subjects.
3. **CENTRANS Sp. z o.o.** with each entity to which it entrusts the processing of personal data shall sign an appropriate agreement (or implement a clause in the master agreement), which comprehensively regulates all issues, procedures and principles of providing personal data for processing.
4. Any personal data may be provided to an external entity for processing only if a personal data processing agreement or an agreement containing a data processing clause is made by both parties.
5. Personal data processing agreements shall be recorded by the Management Board or its GDPR representative.
6. The Company has a model personal data processing agreement.

X. Changes in processing of personal data

1. All personal data processing activities shall be recorded in the register of data processing activities.
2. The register shall be maintained and updated by the GDPR representative, based on information provided from the Company's various departments.
3. The Company has a model register of processing activities.
4. Persons processing personal data at the Company shall notify the GDPR representative immediately of any changes in the way personal data are processed and the amount and type of data processed.

XI. Personal data protection in the planning phase of new developments

1. Persons processing data of the Controller shall take into account the provisions of personal data protection law and all internal regulations of the Controller, including this Personal Data Protection Policy, also in the design phase of new technical solutions or processes, as well as in case of introducing modifications to the already existing solutions and processes.
2. Where a type of processing poses a high risk of infringing the rights or freedoms of individuals, an impact assessment shall first be carried out in accordance with the Data Protection Impact Assessment Procedure (DPIA- the Company has a separate document in this regard) before that type of processing is applied.
3. The Controller shall apply the guidelines of the Polish supervisory authority when identifying operations that may cause a high risk of violation of the rights or freedoms of natural persons.
4. The Controller shall, at each stage, examine whether it is necessary for him/her to appoint a Data Protection Officer.

XII. Archiving

The documentation shall be archived in compliance with legal provisions and internal regulations applicable to the protection of personal data.

XIII. Training

1. Each employee or associate shall undergo, prior to starting his/her work, training on the protection of personal data and the handling of personal data in accordance with the technological and organisational security measures in force at the Company, as well as any laws and guidelines.
2. The GDPR representative shall be responsible for this training.
3. The scope and frequency of the training referred to above shall be adequate to the function performed by individual employees, their responsibilities and the frequency with which they will process and handle personal data.

XIV. Final provisions

1. This Personal Data Protection Policy shall be reviewed by an external Data Protection Officer or an external company dealing with GDPR matters at least once a year.
2. The Personal Data Protection Policy shall be updated when technical or organisational measures to protect personal data are introduced or changed.
3. Once updated, a new version of the Personal Data Protection Policy shall be made and presented to employees and associates for review and the changes made shall be discussed.
4. Failure to comply with the Personal Data Protection Policy, as well as other related documents in force at the Controller, may result in disciplinary actions in accordance with separate regulations.
5. The Personal Data Protection Policy shall come into force as of the date of its execution.
6. The processing of personal data by the Company is subject to the provisions of Polish law, in particular the provisions of the Protection of personal data Act dated May 10th 2018. This Policy may be translated into languages other than Polish, however, in the event of any discrepancies between the language versions, the Polish version will always prevail.