GENERAL PERSONAL DATA PROTECTION POLICY

1. Introduction

1.1 The General Data Protection Regulation of 2016 („GDPR") replaces EU Directive of 1995 on the data protection, replacing at the same time also the legislation of each Member State which was drawn up according to Directive 95/46/CE on the data protection. Its purpose is to protect the rights and freedoms of the natural persons (natural persons alive) and to make sure that the personal data are not processed without their acknowledgement and, whenever necessary, that they are processed with their informative and specific consent.

1.2 Definitions used by Prodal94 (taken from GDPR)
Material scope (Article 2) - GDPR applies to the processing of personal data wholly or partly by automated means (computer, laptop), as well as to the processing other than by automated means of personal data (paper-based registrations) which form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – GDPR applies the processing of personal data in the context of the activities of an establishment of a controller in the EU (European Union), regardless of whether the processing takes place in the Union or not. It applies also to the processing of personal data by a controller not established in the Union, where the processing activities are related to the offering of goods or services or the monitoring of their behaviour as they are established within the Union.

1.3 Article 4 Definitions

Office – the head office of the controller in the EU is the place where the controller makes the main decisions regarding the purposes and means of its data processing activities. The head office of a controller in the EU is where the central management is located. If a controller is established outside the EU, he will have to appoint a representative in the jurisdiction where the controller operates to act on behalf of the controller and deal with the relationship with the surveillance authorities.

Personal data - 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.

Special categories of personal data - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Controller - a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specified criteria for its nomination may be provided for by Union or Member State law.

Data subject – any natural parson alive that is the object of the personal data processing, personal data which are held by an organisation.

Processing - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

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 or to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability or behaviour. This definition is related to the right of the data subject to oppose the creation of profiles and the right to be informed about the existence of such profiles, profile-based measures and the expected effects of profile creation on the individual.

Personal data policy breach - a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed. The controller has the obligation to report the surveillance authorities personal data breaches and cases where the breach could adversely affect the personal data or privacy of the data subject.

Consent of the data subject – means 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.

Child – GDPR defines a child as any person under the age of 16, although this may be reduced to 13 by the Member State law. The processing of the personal data of a child is legal only if the consent of the parents or guardians has been

obtained. The controller makes every reasonable effort to verify in such cases that the parental authority has given its consent.

Third party - a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system - any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralised or dispersed on a functional or geographical basis.

2. Policy statements

2.1 Prodal94 through the members of its management, based in Cernica, 1 C DRUM INTRE TARLALE, Ilfov county, registered with the Trade Register Office under no. J23/881/2002, VAT identification number RO 6646141, undertakes to comply with all relevant EU and Member State laws on personal data and the protection of the rights and freedoms of the persons whose information it collects and processes in accordance with GDPR.

2.2 The compliance with the GDPR is described by this policy and relevant procedures, such as the Procedure on the applications of the data subjects, Procedure on the data security breach, along with related processes and procedures.

2.3 GDPR and this policy are applied to all the personal data processing operations of Prodal94, including those performed on the personal data of the customers, employees, partners and any other personal data that the organization processes from any source.

2.4 The members of the management bodies of Prodal94 designate one or more persons as GDPR Compliance Officer. They do not have the duties of a DPO.

2.5 The GDPR Compliance Officer is involved in the revision of the processing record in the light of any change to the activity of Prodal94 (as determined by the changes to the data inventory and review by the management) as well as any additional requirements identified through data protection impact assessments. This register must be available at the request of the surveillance authority.

2.6 This policy applies to all the employees of Prodal94 as well as to its vendors processing personal data as proxy agents of Prodal94. Any breach of the GDPR or this policy is dealt with in accordance with the Internal Rules of Prodal94, and under the conditions provided by the GDPR, Prodal94 notifies the ANSPDCP of the breach. In the event that the deed causing the breach may also constitute an offense, it will be brought to the attention of the competent authorities as soon as possible.

2.7 The Prodal94 partners which process personal data as proxy agents of Prodal94, must have read, understood and observed this policy. Prodal94 communicates to any such partner this Policy. No third party can process the personal data owned by Prodal94 without having entered into a contract by

which the parties regulate their data privacy obligations. Prodal94 imposes on the third party obligations at least as onerous as those which Prodal94 undertakes.

3. Responsibilities and roles under the General Data Protection Regulation

3.1 Prodal94 is a personal data controller, occasionally acting as a proxy agent under the GDPR.

3.2 The members of the management bodies of Prodal94 are responsible for implementing the necessary measures to ensure the compliance with personal data protection legislation, organizing the personal data processing modality, security management and risks relating thereto, development and encouragement of the good personal data management practices within Prodal94;

3.3 The members of the management bodies of Prodal94 are responsible for the reassessment of the analysis regarding the meeting of the conditions provided by art. 37 paragraph (1) of the GDPR if Prodal94 intends to initiate special data processing or that may have a high risk on the rights and freedoms of the data subjects. Also, a new analysis will be carried out if additional obligations on the personal data protection are introduced under the national law in relation to those laid down in the GDPR.

3.4 The members of the management bodies of Prodal94 will be able to delegate their tasks in the personal data protection field to the GDPR Compliance Officer.

3.5 The GDPR Compliance Officer has a consultative role in procedures such as the Procedure on the applications of the data subjects and is a reference point for employees seeking clarification on data protection issues.

3.6 The compliance with data protection legislation is the responsibility of all Prodal94 employees who process personal data.

3.7 Prodal94 employees are responsible for ensuring that any personal data about them and provided by them to Prodal94 are accurate and up-to-date.

4. Principles on data protection

Any personal data processing must be in accordance with the principles of data protection as set out in Article 5 of the GDPR. Prodal94 policies and procedures are designed to ensure the compliance with the principles**.**

4.1 <u>The personal data must be lawfully, accurately and transparently processed</u>

Lawful – identify a legal basis before processing personal data. These are often referred to as „processing grounds": legal obligation, contract, consent,

legitimate interest of Prodal94, public interest or vital interests of the data subject.

Accurate – In order for the processing to be accurate, the controller must inform the data subjects before staring the processing or as soon as possible. The informing is mandatory regardless of whether personal data has been obtained directly from the data subjects or from other sources.

Transparent – Articles 12, 13 and 14 of the GDPR lay down the rules for informing the data subjects. The provisions are detailed and specific, emphasizing that privacy notifications should be easy to understand and accessible. Information must be communicated to the data subject in an intelligible form using clear and simple language.

The specific information to be provided to the data subject must include at least:

4.1.1 identity and contact details of Prodal94;
4.1.2 purpose of the personal data processing as well as the legal basis of the processing;
4.1.3 storage period of the personal data;
4.1.4 existence of the right to request access, rectification, erasure or opposition to processing and the conditions (or lack thereof) of exercising such right, such as affecting the lawfulness of the previous processing;
4.1.5 categories of the concerned personal data;
4.1.6 recipients or categories of recipients of personal data, as appropriate;
4.1.7 if applicable, Prodal94 intends to transfer personal data to a third-country recipient and the data protection level;
4.1.8 any additional information required to ensure an accurate processing.

4.2 <u>The personal data can only be collected for specific, explicit and legitimate purposes</u>

The data obtained for specific purposes should not be used for a purpose other than the original one, as mentioned in the Processing inventory register owned by Prodal94.

4.3 <u>The personal data must be adequate, relevant and limited to what it is required for processing</u>

4.3.1 The GDPR Compliance Officer can be consulted so that Prodal94 should ensure that it does not collect information that is not strictly necessary to achieve the purpose for which it is obtained.
4.3.2 All forms of (electronic or paper-based) data collection, including the data collection requirements in the new computer systems, must include a correct processing statement or link to the Privacy Policy.

4.3.3 The GDPR Compliance Officer may be consulted in the annual internal/ external audit to determine whether the collected data is still appropriate, relevant and proportionate to the intended purpose.

4.4 The personal data must be accurate and, where necessary, updated by deleting or correcting without delay

4.4.1 The data stored by the controller should be reviewed and updated as appropriate. The data must not be retained unless it can reasonably be assumed that they are accurate.

4.4.2 The GDPR Compliance Officer can participate in the meetings of Prodal94 to ensure that all the personnel are trained on the importance of collecting and maintaining the accurate data.

4.4.3 It is also the responsibility of the data subject to ensure that the data held by Prodal94 is accurate and up-to-date. The completion of a registration form or application by a data subject will include a statement that the data contained therein is correct on the filing date.

4.4.4 The employees and representatives of Prodal94 must notify the collector of any changes to their personal data to allow the personal data record to be updated properly. It is the responsibility of Prodal94 to ensure that any change in status notification is recorded and taken into account.

4.4.5 At least annually, the GDPR Compliance Officer verifies the waiver terms for all the personal data processing performed by Prodal94 and recorded in the Data Processing Register and identifies any data processing and/ or data categories that are no longer necessary in the context of the registered purpose. These data will be safely deleted/ destroyed only as a result of the decision of Prodal94.

4.4.6 Prodal94 has the responsibility to respond to the requests for rectification from the data subjects within 30 days (Procedure on the applications of the data subjects). The deadline can be extended by up to two months for complex requests. If Prodal94 decides not to comply with the request or to extend the period for replying, it must inform the data subject of the reasons underlying that decision as well as of his/ her right to lodge a complaint with the surveillance authority.

4.5 The personal data must be kept in a form that allows the identification of the data subject only for as long as it is necessary for processing.

4.5.1 If the personal data is kept beyond the processing date, these are pseudonymized to protect the identity of the data subject in the case of a data security breach.

4.5.2 The personal data are retained throughout the processing by each Department that holds them, and the Department managers are responsible for deleting/ destroying the personal data if the preservation period is exceeded.

4.5.3 The GDPR Compliance Officer can be consulted on any preservation of data beyond the defined preservation periods and Prodal94 must

ensure that the justification is clearly identified and complies with the requirements of the data protection legislation.

4.6 The personal data must be processed in a way that ensures proper security
The GDPR Compliance Officer is consulted on the risk assessment taking into account all the circumstances of Controlling or Processing operations of Prodal94.

In order to determine the appropriateness, it may be consulted also the GDPR Compliance Officer, that should also consider the extent of any damage or loss that might be caused to data subjects (e.g. staff or customers) if a security breach occurs, the effect of any security breach on Prodal94 itself, and any possible reputational damage, including possible loss of customer confidence.

When evaluating the appropriate technical measures, Prodal94 considers the following:

- Password protection with a minimum complexity degree of *[8]* alphanumeric characters;
- Automatic lock of the inert terminals after *[1/3/5]* minutes;
- Removal or monitoring of the access rights for USB and other storage media;
- Antivirus software and firewall;
- Access rights based on job tasks, including those assigned to temporary staff;
- Encryption of the devices leaving the premises of the organization, such as laptops;
- LAN (Local Area Network) and WAN (Wide Area Network) security;
- Privacy Enhancement Technologies, such as pseudonymization and anonymization;

When assessing appropriate organizational measures, Prodal94 considers the following:

- Appropriate training levels for all employees;
- Employees sign a commitment to personal data protection. Inclusion of these obligations in the Internal Regulations;
- Identification of disciplinary sanction measures for breaching data security;
- Monitoring staff on established security obligations;
- Controls regarding the physical access to electronic and paper-based records (for example, access rights in applications);
- Paper-based data storage in secure cabinets (at least under key lock);

- Restricting the use of portable electronic devices outside the workplace or defining clear rules on their use;
- Restricting the use of the employee's personal devices at the workplace;
- Adoption of clear rules on passwords.

4.7 The collector must be able to demonstrate the compliance with the other GDPR principles (responsibility)

According to art. 5 paragraph (2) of the GDPR, Prodal94 complies with the data protection principles by implementing data protection policies, technical and organizational measures, and adopting some techniques such as data protection by design (privacy by design), impact analysis, infringement notification procedures and incident response plans.

5. Rights of the data subjects

5.1 The data subjects have the following rights regarding the data processing:

- 5.1.1 Right of access - through which a confirmation can be obtained from Prodal94 that his/her personal data is processed or not.
- 5.1.2 Right to rectification - this implies the possibility of asking Prodal94 to correct inaccurate data concerning them;
- 5.1.3 Right to be forgotten - through which s/he can obtain the deletion of his/her data by Prodal94, under certain conditions provided in the GDPR;
- 5.1.4 Right to restrict processing - occurs in the case of inaccurate, unlawful processing or exercise of the right to object by the data subject;
- 5.1.5 Right to data portability - the right to receive the personal data concerning him/her and which Prodal94 has provided in a structured, commonly used and readable format, including the right to transmit this data to another collector;
- 5.1.6 Right to oppose - including the right to oppose the creation of profiles.
- 5.1.7 Right to information - implies informing the data subjects in a concise, transparent and easily accessible manner about the processed data.
- 5.1.8 The right to address a complaint to the Surveillance Authority.

5.2 Prodal94 ensures that the data subjects can exercise these rights:

- 5.2.1 The data subjects can file applications for access to the data as described in the Procedure on the applications of the data subjects.
- 5.2.2 The data subjects have the right to complain to Prodal94 about the processing of their personal data.

6. Consent

6.1 Prodal94 understands "consent" as being granted through an unequivocal act which is a freely expressed, specific, informed and clear expression of the data subject's consent to the processing of his/her personal data. The data subject may withdraw his/her consent at any time.

6.2 The consent obtained under pressure or on the basis of misleading information is not a valid basis for processing.

6.3 There must be evidence of communication between the parties to demonstrate the expressed consent of the data subjects. The consent cannot be deduced from a lack of response to a notification. The collector must be able to demonstrate that the consent has been obtained for the processing operation.

6.4 For the processing of sensitive data, the explicit written consent (Procedure of granting the consent) of the data subjects must be obtained, unless there is another legal basis for processing.

6.5 If the consent to process personal and sensitive data is the legal basis of the processing, this is acquired by Prodal94 using the Procedure of granting the consent.

7. Data security

7.1 All employees must ensure that any personal data that Prodal94 holds and for which they are responsible are safely stored and are in no way disclosed to any third party unless this third party has been authorized specifically by Prodal94 to receive this information.

7.2 All personal data should only be accessible to those who need to use them in accordance with the access rights. All personal data must be handled safely and must be kept:

- in a closed room with controlled access; and/or
- in a locked drawer or cabinet; and/or
- if computerized, password-protected according to the security level established by Prodal94; and/or
- stored on a (removable) media that is encrypted.

7.3 Prodal94 employees ensure that the screens of the devices they use are not visible to any unauthorized third party. All employees must conclude a User Agreement Commitment.

7.4 The physical documents, as well as any copies thereof must not be left in places accessible to unauthorized personnel and may not be used outside the head offices or the place where they are stored without explicit authorization. Any copy must be destroyed as soon as the purpose for which it was carried out has been accomplished.

7.5 The physical documents for which the established deletion deadline has been met must be disposed of and destroyed as "confidential waste".

7.6 Before disposing of the electronic devices, their storage media must be reset to factory settings or destroyed.

7.7 The processing of the personal data outside Prodal94 presents a potentially greater risk of loss, theft or damage of the personal data. Employees must be specifically authorised to process off-site data.

8. Disclosure of data

8.1 Prodal94 must ensure that personal data is not disclosed to unauthorized third parties. Employees are aware that family members and/or friends are included in the category of unauthorized third parties.

9. Data preservation and disposal

9.1 Prodal94 does not preserve personal data in a form that allows the identification of the data subjects for a longer period than is necessary in relation to the purpose(s) for which the data was originally collected.

9.2 Prodal94 may store data for longer periods if the personal data is processed exclusively for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes to implement the appropriate technical

and organizational measures in order to protect the rights and freedoms of the data subject.

9.3 The personal data must be safely disposed of in accordance with the sixth principle of the GDPR - processed in an appropriate manner to maintain the security, thus protecting the "rights and freedoms" of the data subjects**.**

10. Data transfers

10.1 The transfer of personal data outside the EEA is prohibited unless one or more specified safeguards or exceptions apply:

10.1.1 A adequacy decision

The European Commission can and will assess third countries, a territory and/or certain sectors of third countries to assess whether there is an adequate level of protection of the rights and freedoms of the individuals.

In these cases, no authorization is required.

The countries that are members of the European Economic Area (EEA), but not the EU, are accepted as meeting the conditions of a adequacy decision.

A list of the countries currently meeting the Commission's adequacy requirements is published in the *Official Journal of the European Union*. *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*

10.1.2 Privacy Shield

If Prodal94 wants to transfer personal data from the EU to a US organization, it should check if the organization is registered with the Privacy Shield of the US Department of Commerce. The US DOC is responsible for managing and administrating the data protection system and ensuring the compliance by companies. In order to be able to certify, the companies must have a privacy policy in accordance with the privacy principles, e.g. personal data use, storage and transfer in accordance with a strong set of rules and data protection safeguards. The protection of the personal data applies regardless of whether the personal data relates to an EU or a non-EU resident. The organizations must renew their "membership status" in the Privacy Shield every year, and if they do not, they can no longer receive and use personal data from the EU under this framework.

Adequacy assessment by the collector

When assessing the adequacy, the collector must take into account the following factors:

- nature of the transferred information;
- country or territory of origin and the final destination of the information;

- way how the information is used and for how long;
- laws and practices of the country of transfer, including the relevant practice codes and international obligations; and
- security measures to be taken with respect to the data from the foreign location.

10.1.3 Mandatory corporate rules
Prodal94 may adopt its own rules for the data transfer outside the EU. These require the prior approval of the competent Surveillance Authority.

10.1.4 Exceptions
In the absence of an adequacy decision, membership of the Privacy Shield, mandatory corporate rules, the personal data transfer to a third country or to an international organization occurs only under the following conditions:

- the data subject explicitly agreed to the proposed transfer after having been informed of the possible risks of such transfers for the data subject due to the lack of an adequacy decision and appropriate security measures;
- the transfer is necessary for the carrying out of a contract between the data subject and the collector or for the carrying out of pre-contractual provisions adopted at the request of the data subject;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the collector and another natural or legal person;
- the transfer is necessary for important public interest reasons;
- the transfer is necessary for the establishment, exercise or defence of the legal claims; and/or
- the transfer is necessary to protect the vital interests of the data subject or other persons if the data subject is not physically or legally capable of giving his/her consent.

11. Personal data processing register

11.1 Prodal94 carried out a data inventory and a Personal data processing register as part of its GDPR Compliance Project.

11.2 Prodal94 is aware of any risks related to the processing of certain types of personal data.

11.2.1 Prodal94 assesses the level of risk related to the processing of personal data for the data subjects. The impact assessments on the data protection are carried out in connection with the processing of the personal data by Prodal94, and in connection with the processing carried out by other organizations on behalf of Prodal94.

11.2.2 Prodal94 manages any identified risks through analyses to reduce the likelihood of breaching the provisions on personal data protection.

11.2.3 Given the nature, scope, context and purposes of the processing, if a type of processing, especially that based on the use of new technologies, is likely to create a high risk for the rights and freedoms of individuals, Prodal94 performs, before processing, an impact analysis of the stipulated processing operations on the personal data protection. A single analysis can address a set of similar processing operations that present equally high risks.

11.2.4 If the outcome of a DPIA shows that such personal data processing could cause harm to the data subjects, Prodal94 applies the prior consultation procedure referred to in Article 36 of the GDPR.

Responsible and approved

The Executive Director is the holder of this document and is responsible for ensuring that this policy document is reviewed in accordance with the above-mentioned review requirements.

A current version of this document is available to all the personnel members on *[Intranet Prodal94]* and is published on *www.stalinskaya.com*

This policy was approved by Prodal94 Management on *24.05.2018* and is issued based on a controlled version under the signature of the Executive Director (CEO).